

CHAPITRE 1

INITIATION AUX RÉSEAUX COMMUTÉS

Auditoire : D-LCS GLSI, IM

Objectifs

- Décrire la convergence des données, de la voix, la vidéo et dans le contexte des réseaux commutés
- Décrire un réseau commuté de PME
- Expliquer le processus de transfert de trames dans un réseau commuté
- Comparer un domaine de collision à un domaine de diffusion

Conception des réseaux

■ La conception de réseau consiste à planifier l'infrastructure d'un réseau informatique.

■ La conception d'un réseau est nécessaire car chaque entreprise a des exigences particulières pour son réseau informatique.

- 1) Identifier les différentes exigences du réseau (taille de l'entreprise et des opérations effectuées...)
- 2) Choisir les périphériques et les équipements nécessaires (nombre et types...)
- 3) Cartographier les connexions du réseau (vérifier les connexions qui devront être établies)
- 4) Assurer une implémentation réussie (mécanismes de de sécurité, outils de surveillance...)

Réseaux convergents

Réseaux de nouvelle génération

- Prendre en charge le matériel moderne, tout en intégrant des plates-formes traditionnelles
- Certains anciens périphériques encore couramment utilisés, qui doivent souvent être incorporés à la conception d'un réseau.

Composants hérités



Petits systèmes PBX



Grands commutateurs téléphoniques



Infrastructure de local technique

Composants de réseau convergent



Communications unifiées - serveur de convergence de support



Commutateurs de base de LAN Cisco Catalyst 2960-S



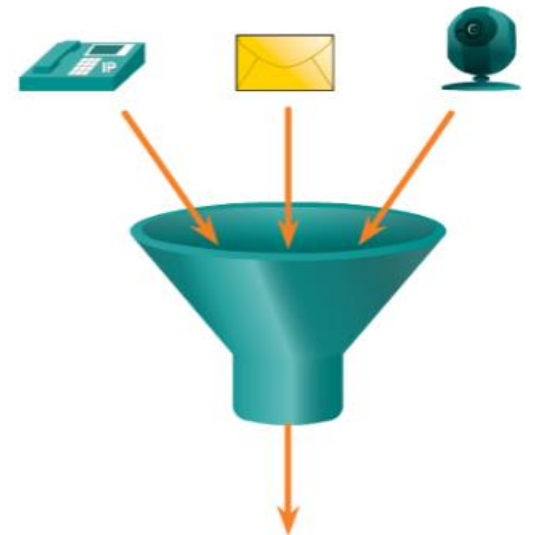
Téléphones IP Cisco Unified

Anciens périphériques encore couramment utilisés (incorporés)

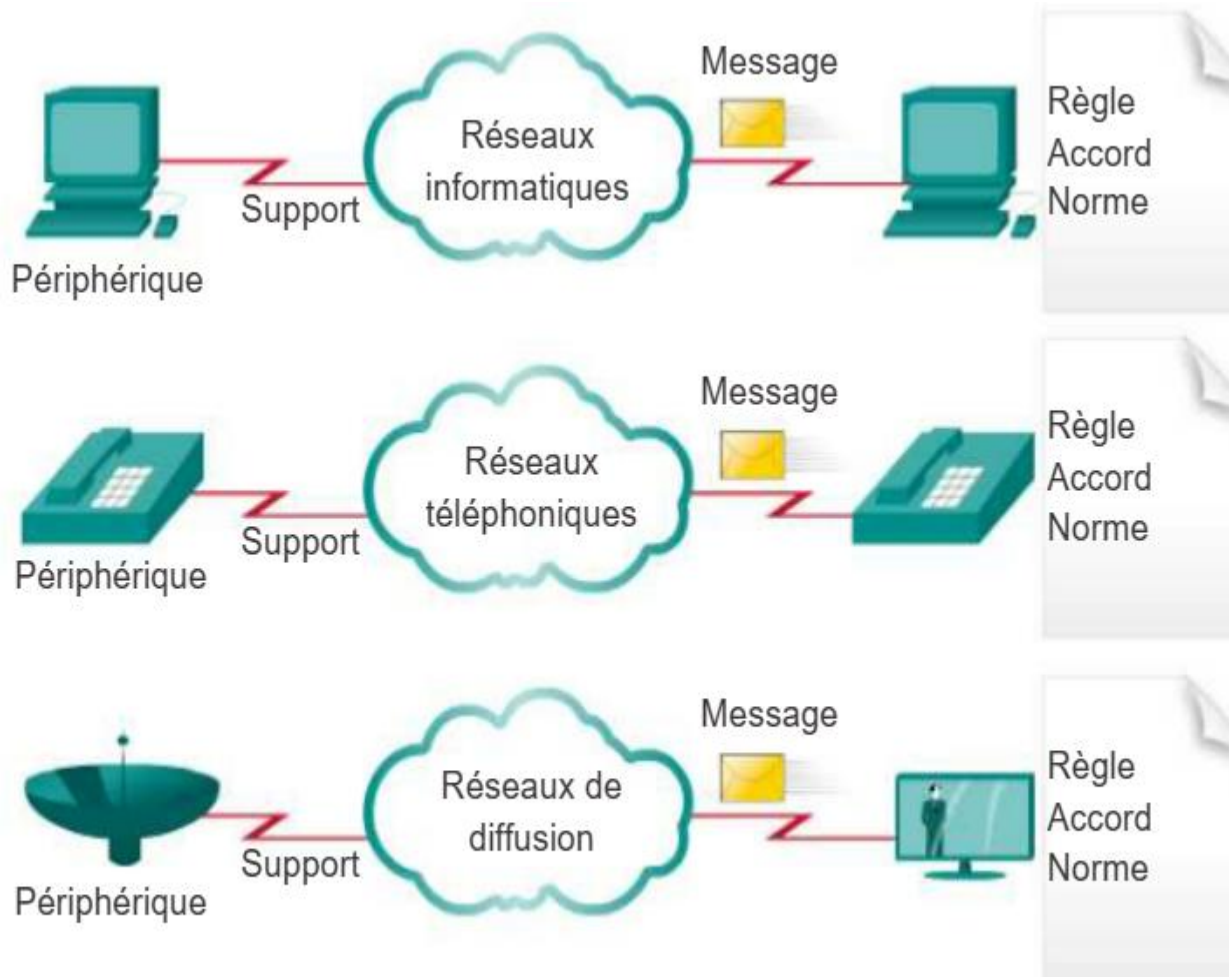
Plates-formes plus récentes

Réseaux convergents

- La collaboration est une exigence
- les réseaux d'entreprise ont recours à des solutions convergentes
- Services de données tels que les systèmes vocaux, les téléphones IP, les passerelles voix, la prise en charge de la vidéo et les vidéoconférences
- Inclut les fonctionnalités :
 - Contrôle d'appels : mise en attentes, transfert d'appels
 - Standards automatisés
 - Mobilité : réception d'appels important de tout lieu



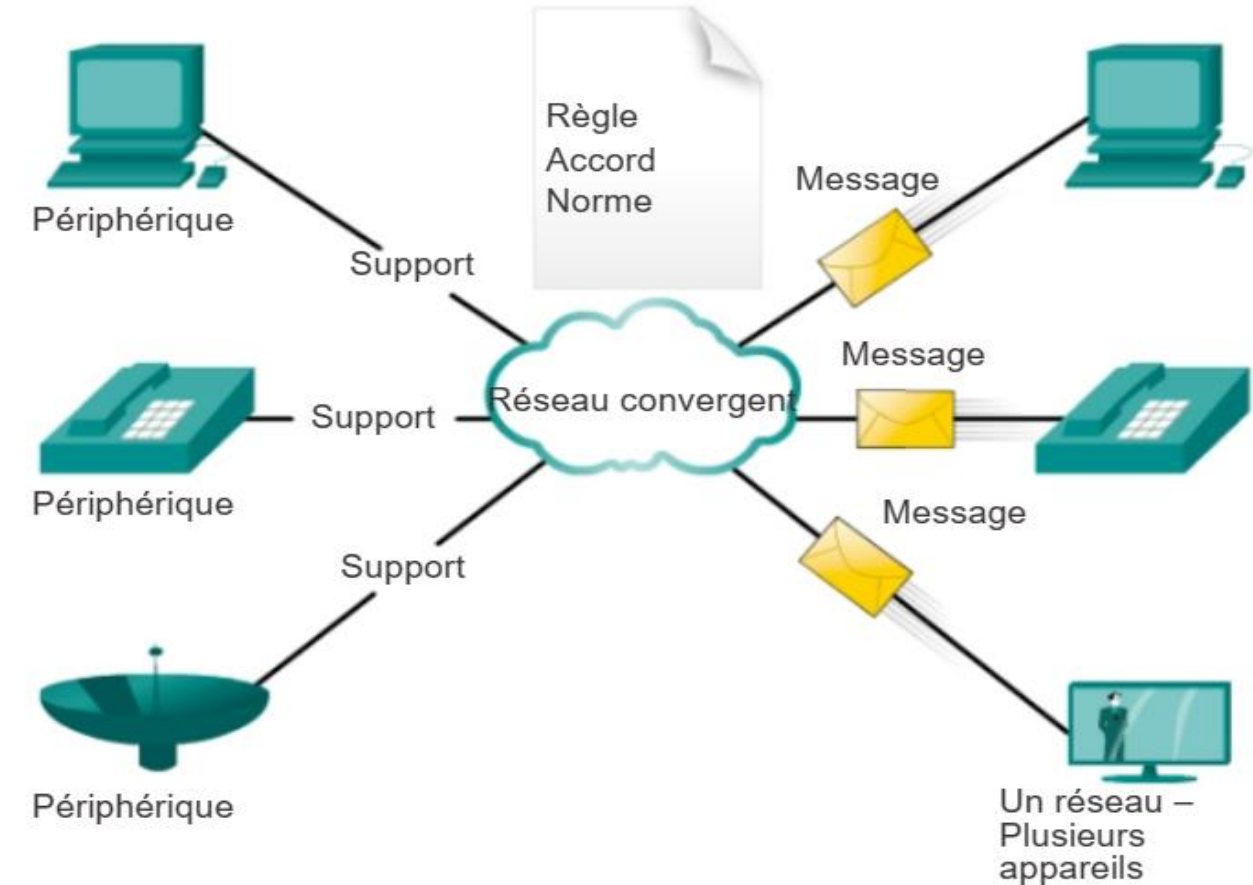
Réseaux classiques



Plusieurs services s'exécutent sur plusieurs réseaux.

Ces réseaux séparés nécessitent chacun une technique différente pour le transport de son service

Réseaux convergents



Les réseaux de données convergents exécutent plusieurs services sur un même réseau.

Une seule infrastructure réseau utilise le même ensemble de règles, de contrats et de normes de mise en œuvre

Réseaux convergents

- La convergence a pour objectif de regrouper le maximum de fonctionnalités en utilisant un minimum de canaux et de transcodeurs
- Le concept convergence repose sur la numérisation des informations relatives à différentes catégories de service (en particulier : téléphonie, informatique, audiovisuel), ce qui permet ensuite de traiter ces informations relatives avec des systèmes communs et de les transmettre sur des réseaux communs

Réseaux convergents

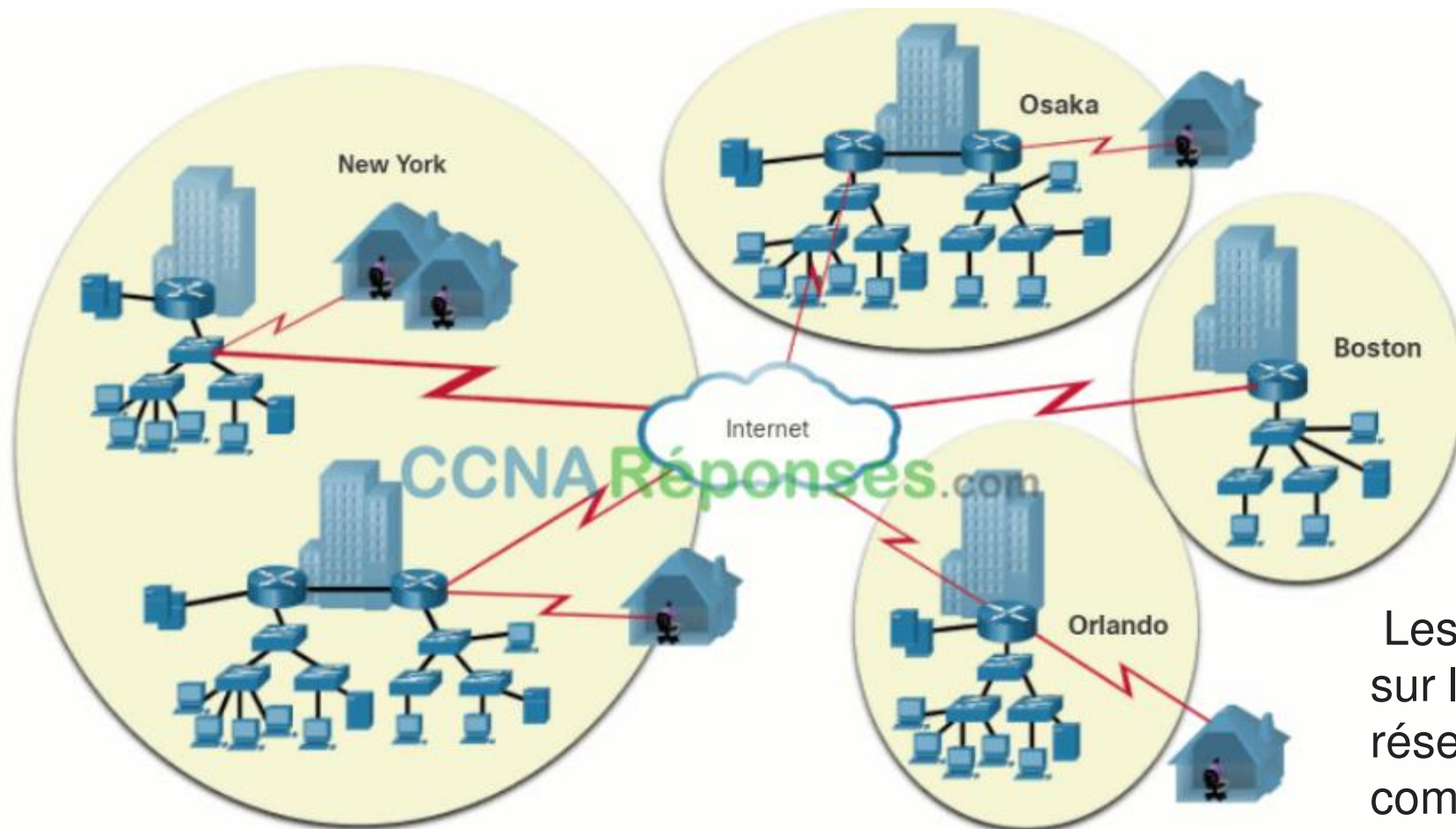
■ Avantages

- Plusieurs types de trafic, un seul réseau à gérer
- Des économies considérables sur l'installation et la gestion des différents réseaux (voix, vidéo, données)
- Gestion informatique intégré

Réseaux commutés

- Le terme commuté vient du fait que les communications sont rendues possibles grâce à des commutateurs automatiques, dispositifs assurant une liaison temporaire entre **deux** équipements.
- Ces commutateurs délivrent une bande passante fixe
- Contrairement aux réseaux **concentrés** qui délivrent une bande passante partagée entre les utilisateurs.
- Équipements sont « *plug and play* » → mise en réseau rapide ne nécessite pas de connaissances particulières.
- Protocole : **Ethernet IEEE 802.3** (ancien)
Ethernet II, (récent)

Réseaux commutés sans frontière



L'entreprise s'étend à d'autres pays.

Remarque : Tous les réseaux d'entreprise ne sont pas internationaux.

Les conceptions de réseaux sur les campus vont des petits réseaux utilisant un seul commutateur LAN à des très grands réseaux comptant des milliers de connexions.

Réseaux commutés sans frontière

- Le réseau sans frontières de Cisco est une architecture réseau qui permet aux entreprises de connecter n'importe qui, n'importe où, à tout moment et sur n'importe quel appareil d'une manière à fois **sûre**, **fiable** et **transparente**
- Il est conçu pour répondre aux besoins des services informatiques et des entreprises, notamment en matière de prise en charge du réseau convergent et les nouvelles façons de travailler

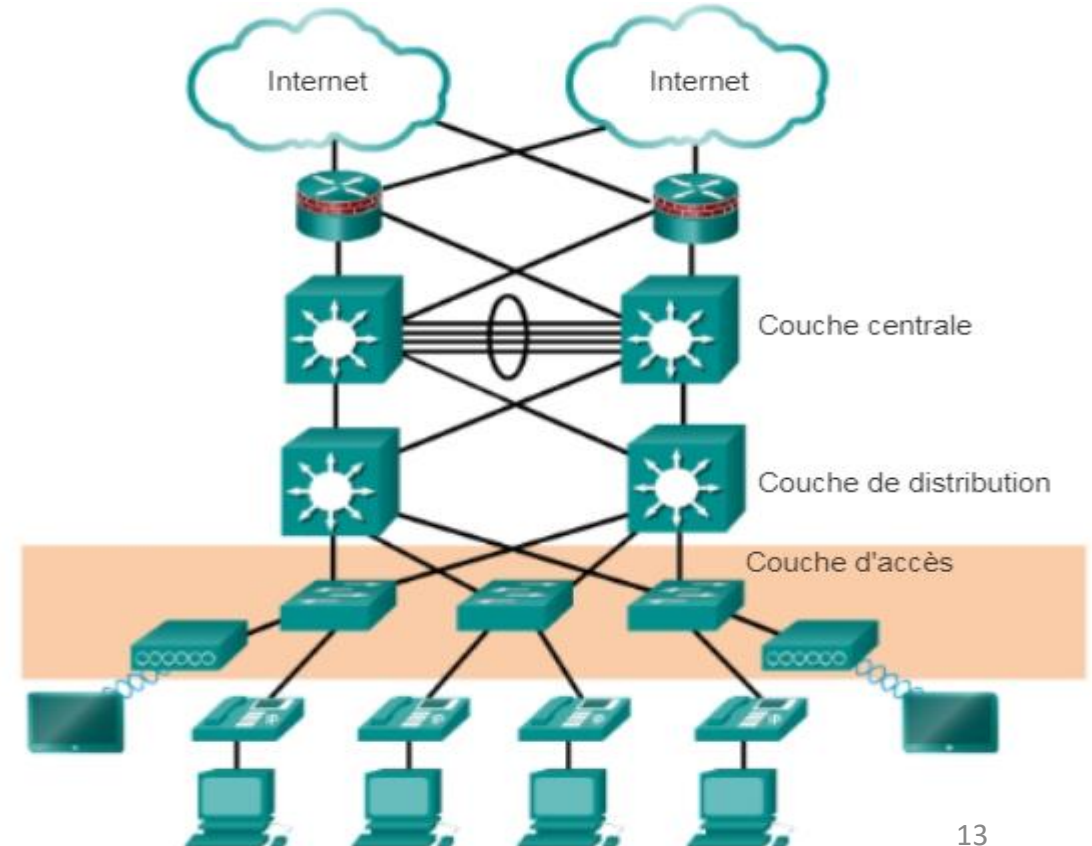
Réseaux commutés sans frontière

- Dans la conception de réseau, il est utile de classer les réseaux en fonction du nombre de périphériques gérés:
 1. **Petit réseau** : fournit les services pour environ 200 périphériques.
 2. **Réseau moyen** : fournit les services de 200 à 1000 périphériques.
 3. **Grand réseau** : fournit les services au-delà de 1000 périphériques.
- Lors de la conception d'un réseau, de nombreuses variables sont à prendre en considération.
- Cisco Certified Design Associate (CCDA®) est une certification reconnue pour les ingénieurs, les techniciens et les ingénieurs supports impliqués dans la conception de réseaux.

Réseaux commutés sans frontière

■ Les directives de conception de réseaux commutés sans frontières reposent sur les principes suivants :

- Hiérarchique
- Modularité
- Résilience
- Flexibilité



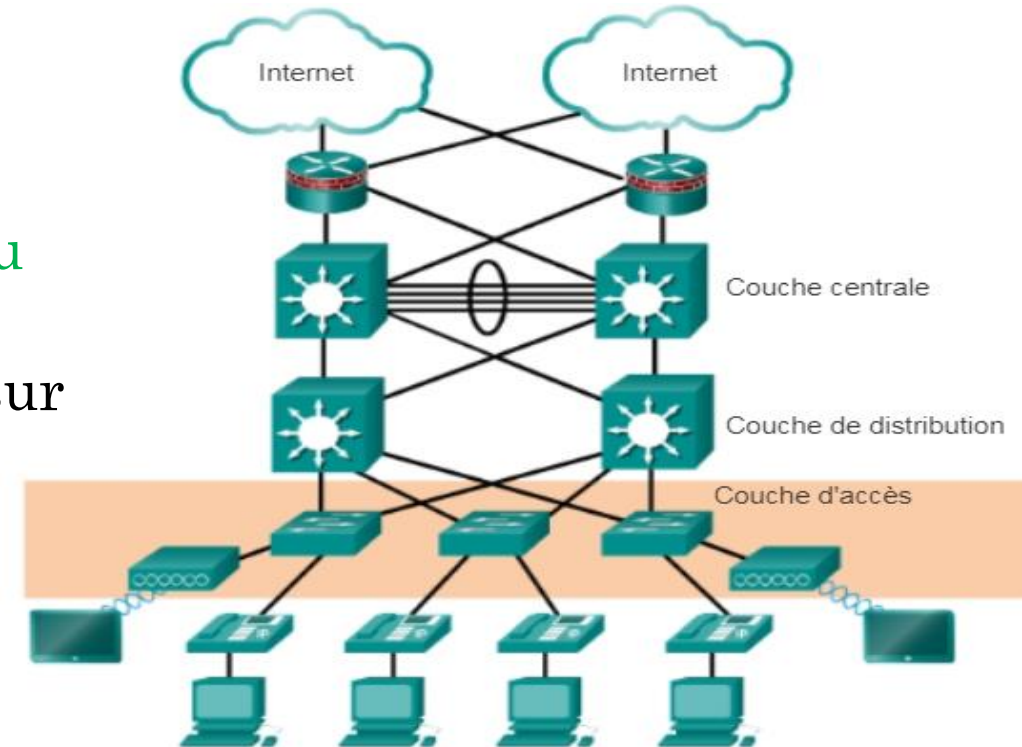
Réseaux commutés sans frontière

- **Hiérarchie** : ce principe décompose le problème complexe que pose la conception du réseau en **plus petits éléments**.
- **Modularité** : permettre l'extension transparente du réseau et l'activation de services intégrés à la demande → conception du réseau **plus simple**. Cisco a identifié plusieurs modules, dont le **compus d'entreprise**, le **bloc de services**, le **data center** et la **périphérie d'Internet**
- **Résilience** : le réseaux **doit** rester **disponible et utilisable** dans des conditions **normales** et **anormales**
 1. Conditions **normales** → événements **prévus**, exemple périodes de maintenance.
 2. Conditions **anormales** → événements **non prévus**, exemple pannes **DoS** (Deny of Service)
- **Flexibilité** : utiliser toutes les ressources du réseau, afin de répartir avec intelligence la charge de trafic → ajouter de **nouveaux services** sans avoir à passer par une **mise à jour complexe**,

Réseaux commutés sans frontière

La conception du réseau permet au concepteur et à l'architecte de sélectionner le matériel et les logiciels réseau adaptés

1. Couche d'accès- permet aux utilisateur d'accéder au réseau
2. Couche distribution- fournit la connectivité basée sur des stratégies,
3. Couche cœur de réseau- assure le transport rapide entre commutateurs de distribution



Le modèle hiérarchique applique à la fois les conception LAN et WAN

Réseaux commutés sans frontière

- **Couche d'accès** La couche d'accès constitue la périphérie du réseau, où le trafic **entre** dans le **réseau de campus** et en **sort**. Traditionnellement, un commutateur de couche d'accès a pour fonction principale de fournir à l'utilisateur un accès au réseau.

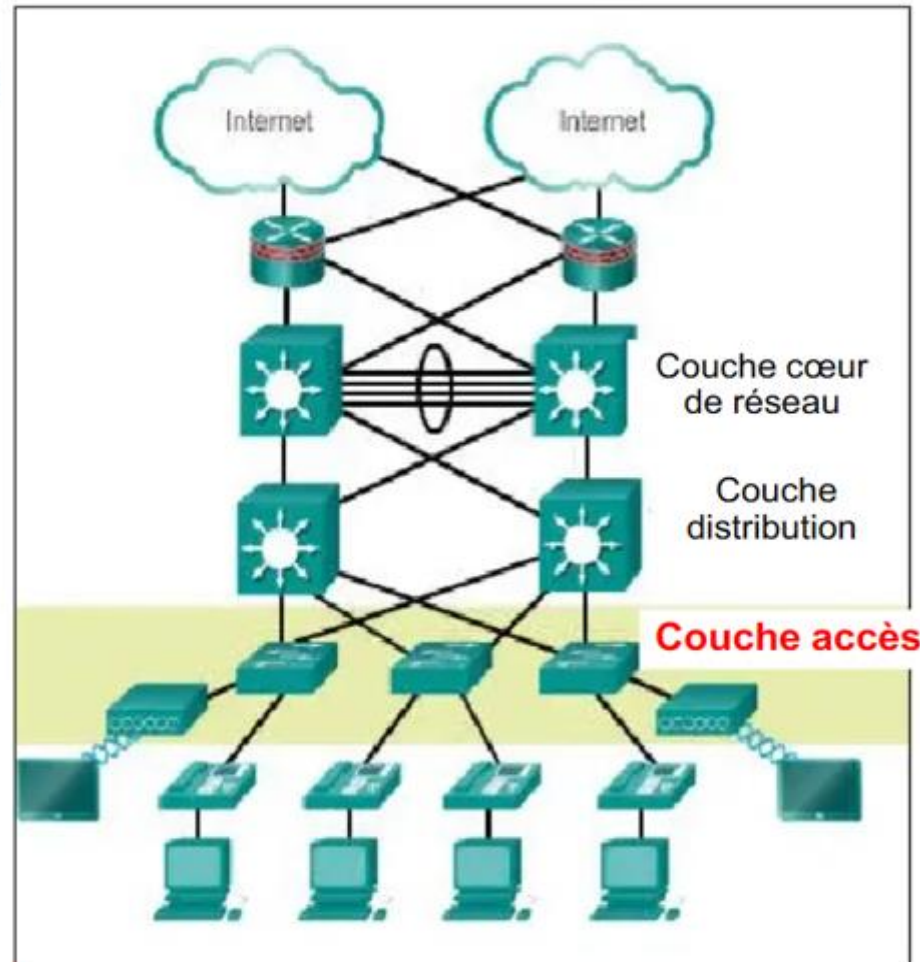
Les commutateurs de couche d'accès se connectent aux commutateurs de la couche de distribution.

Ceux-ci implémentent des technologies de fondation de réseau telles que le routage, la qualité de service et la sécurité.

Réseaux commutés sans frontière

■ La **couche d'accès** a plusieurs fonctions:

1. Commutation de **couche 2**
2. Disponibilité **élevée**
3. **Sécurité** des ports
4. **Classification** de la **QoS** et **limite** de **contrôle**.
5. Inspection du **Address Resolution Protocol (ARP)**



Ports d'accès sont les ports de commutation qui se connectent **aux points d'extrémité Ethernet**.

Sécurité des ports

Inspection ARP

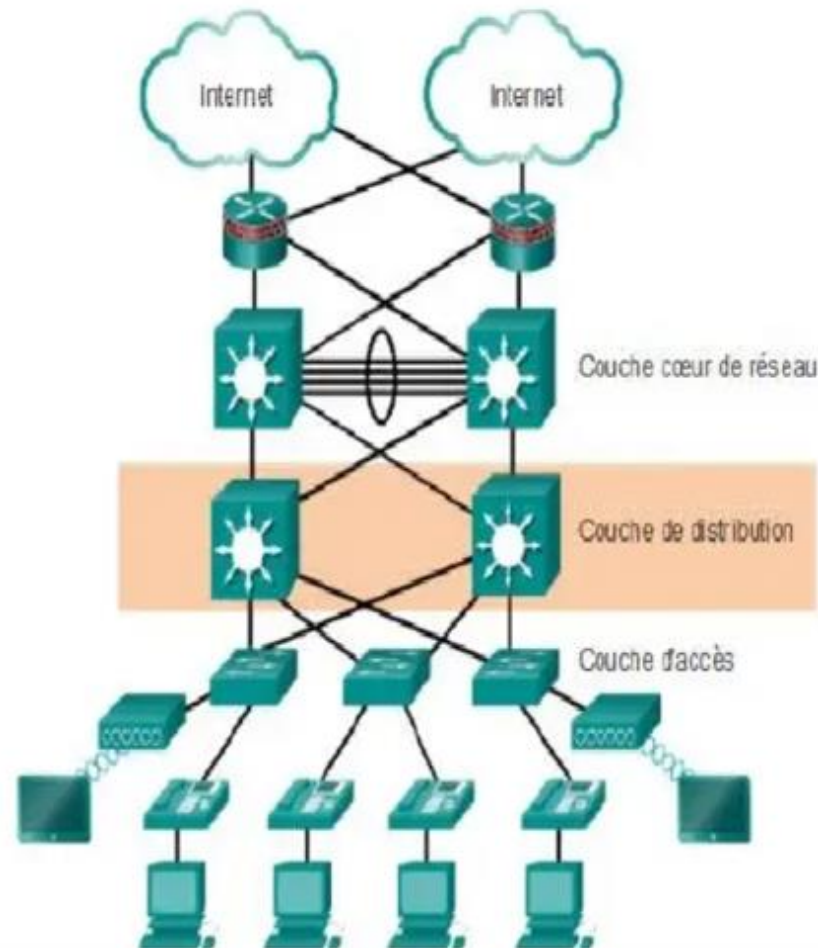
Surveillance DHCP

Limitation des @ MAC

Réseaux commutés sans frontière

La couche de distribution

- Agrégation des liaisons LAN ou WAN
- Sécurité basée sur des stratégies sous forme d'ACLs et de filtrage
- Services de routage entre LAN et VLAN, et entre domaines de routage, exemple EIGRP vers OSPF.
- Redondance et l'équilibrage de charge .



Sécurité des ports

- Configuration de VLAN
- listes de contrôle d'accès (ACLs)

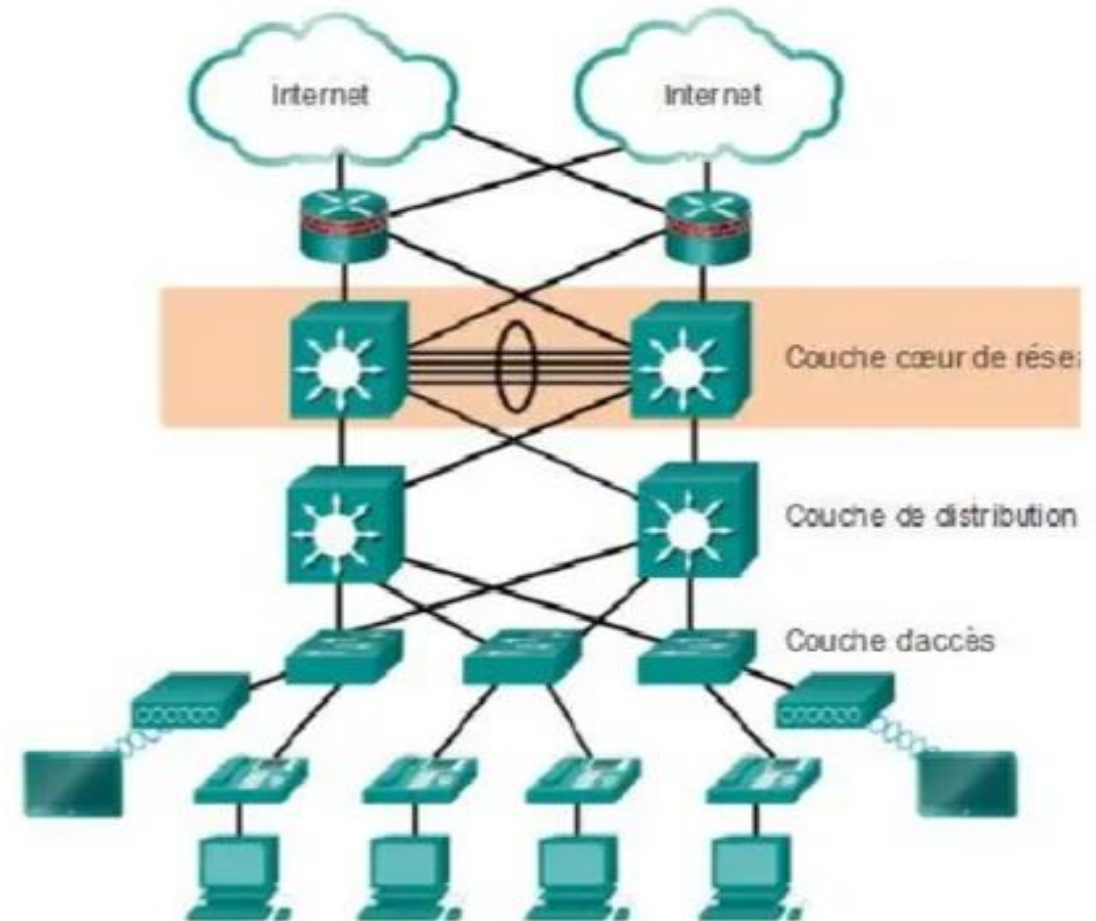
Réseaux commutés sans frontière

- **Couche de distribution** La couche de distribution établit l'interface entre la couche d'accès et la couche cœur de réseau pour fournir de nombreuses fonctions importantes, notamment :
 - Regroupement de réseaux étendus d'armoires de câblage
 - Regroupement des domaines de diffusion de couche 2 et des limites de routage de couche 3
 - Fonctions intelligentes de commutation, de routage et de règles d'accès au réseau, pour l'accès au reste du réseau
 - Haute disponibilité pour l'utilisateur final et **chemins à coût égal** vers le cœur de réseau au moyen de commutateurs redondants dans la couche de distribution
 - **Services différenciés**, pour différentes classes d'applications de services à la périphérie du réseau

Réseaux commutés sans frontière

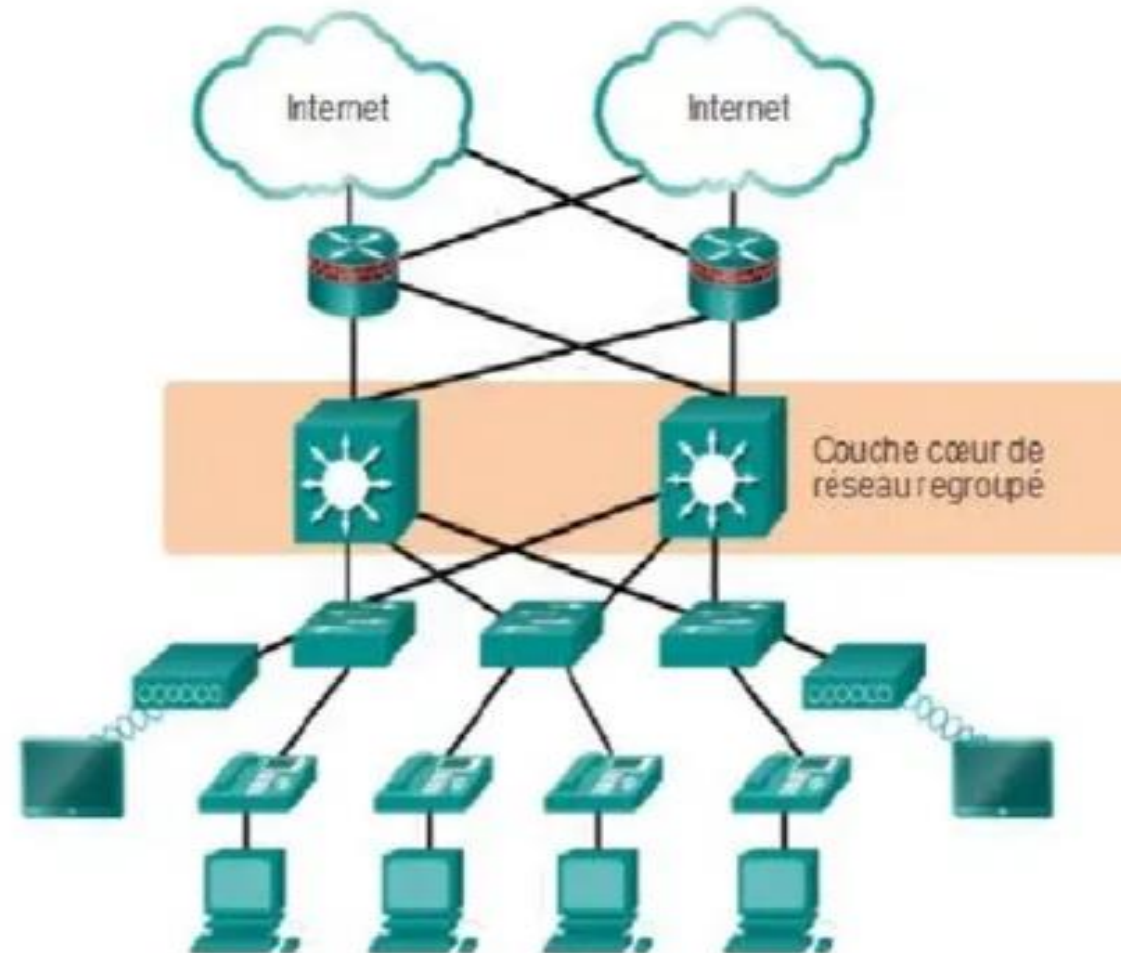
La couche de cœur

- Elle se compose de **périphériques réseau à grande vitesse**, par exemple les **Cisco Catalyst 6500** ou **6800**.
- **Commutation haute vitesse** (transport rapide)
- **Fiabilité** et **tolérance** aux **pannes**
- **Mise à l'échelle** avec un **équipement plus rapide**,



Réseaux commutés sans frontière

- On parle de **cœur de réseau regroupé** lorsque les **fonctions** de couche de **distribution** et de couche **cœur de réseau** sont **mises en œuvre sur un seul périphérique**.



Réseaux commutés sans frontière

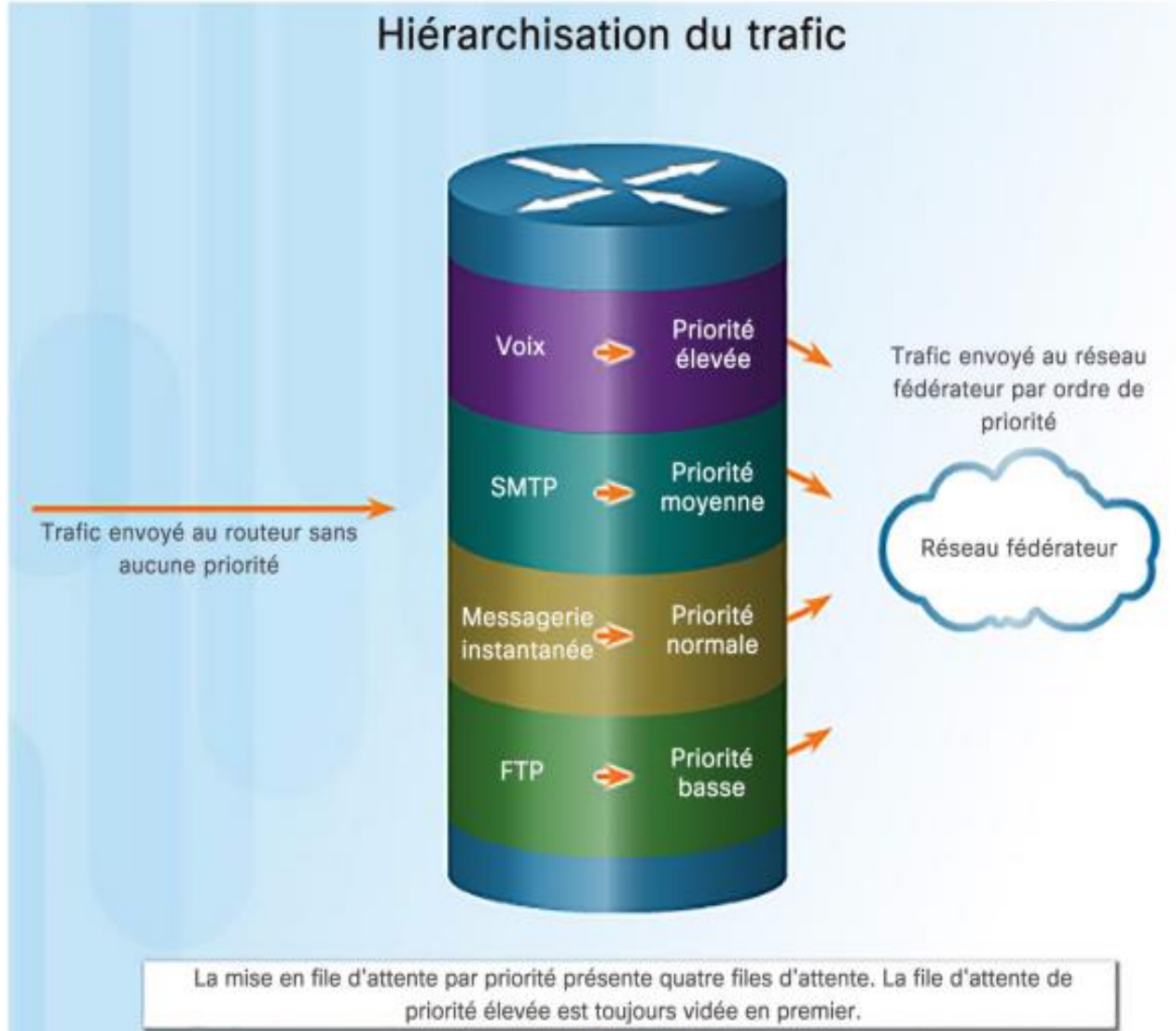
- **Couche cœur** La couche cœur de réseau sert de réseau **fédérateur** Elle connecte plusieurs couches du réseau de campus. La couche cœur de réseau sert d'agrégateur pour tous les autres blocs de campus et joint le campus au reste du réseau.

La couche cœur de réseau a pour objectif principal d'assurer l'isolation des défaillances et la connectivité haut débit du réseau fédérateur.

Réseaux commutés(Qualité de Service)

- Qualité de Service (QoS),
- Besoin du réseau capable de différencier plusieurs types de trafic.
- Les mécanismes de **différenciation de service** doivent être implémentés de bout en bout, c'est-à-dire de l'ordinateur de bureau jusqu'au cœur du réseau et inversement.
- A la périphérie du réseau local, la qualité de service peut être mise en œuvre au niveau des commutateurs (niveau 2). Analyser les trames entrantes, afin de les **classer** et de les introduire dans la **file d'attente** appropriée, en fonction du **degré de priorité accordé**.
La retransmission des trames les plus **urgentes** est ainsi **prioritaire**.

Réseaux commutés : Qualité de Service



- Les types de trafic et la façon dont ils devront être gérés doivent être pris en compte et considérés comme une priorité dans la conception du réseau.
- Dans un réseau de petite taille, les routeurs et les commutateurs doivent être configurés pour prendre en charge le trafic en temps réel, comme la voix et la vidéo. Par exemple :
 - Voix → Haute priorité
 - Vidéo → Haute priorité
 - SMTP → Priorité moyenne
 - Messagerie instantanée → Priorité normale
 - FTP → Priorité basse
- Le trafic réseau doit être classé en fonction des priorités afin d'améliorer la productivité des employés et d'en limiter les interruptions de fonctionnement.

Réseaux commutés

Qualité de Service

Tous les commutateurs savent offrir un service de **bout en bout**.

l'architecture **DiffServ** (Differentiated Services ou services différenciés) :

- Différencier les flux selon plusieurs critères dont **l'adresse IP** ou le **flux applicatif** (http, mail...)
- Quatre étapes de **mécanisme de QoS** proposées par commutateurs CISCO
 - 1) la classification des trames,
 - 2) leurs comparaisons avec des profils prédéfinis,
 - 3) le marquage des trames correspondant à un certain profil (priorité)
 - 4) leur mise en files d'attente (traiter par algorithmes d'ordonnancement)

Réseaux commutés

- Le rôle des réseaux commutés a évolué :
 - Un réseau local (LAN) commuté accroît la **flexibilité** et permet la **gestion du trafic**
 - Il prend également en charge des fonctionnalités telles que la **qualité de service**, la **sécurité** renforcée, la prise en charge de la technologie sans fil et de la téléphonie IP, et les services de mobilité

Commutation LAN

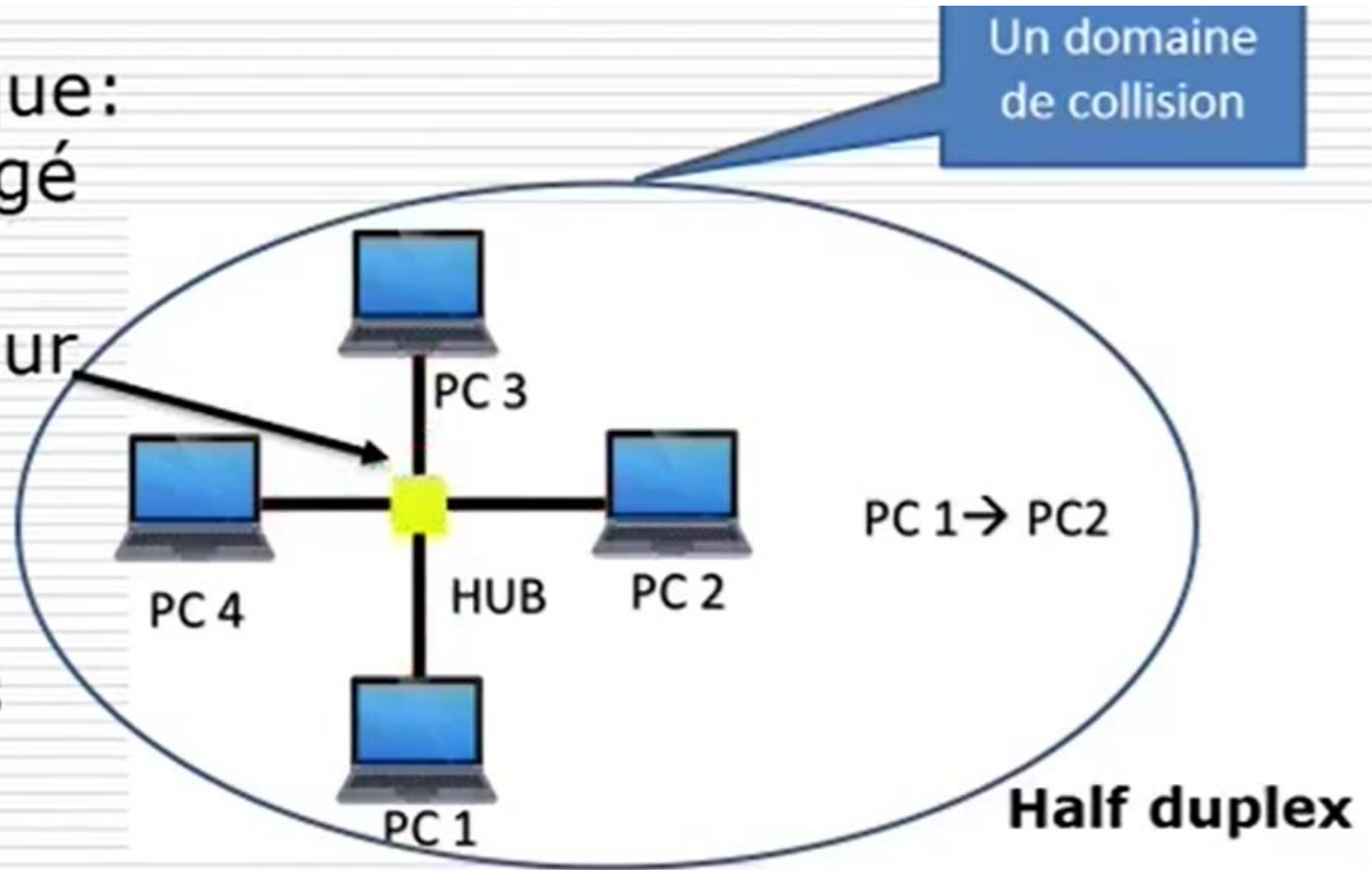
Problèmes avec un LAN classique

➤ Ethernet classique:

- Média partagé
- CSMA/CD
- Concentrateur

➤ Problèmes:

- Collisions
- Congestions
- Latence
- Broadcast



Commutation LAN

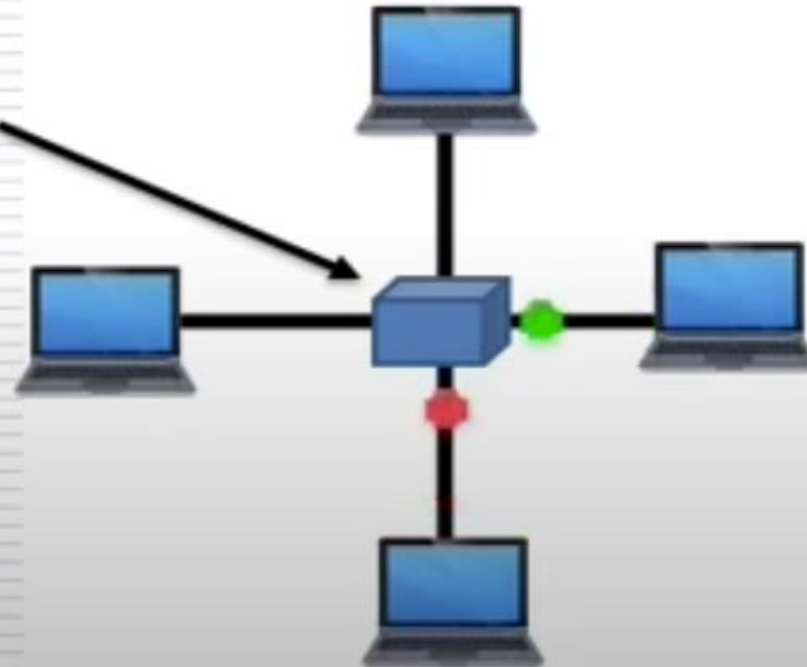
Solution : Ethernet commuté

➤ Solutions

- Segmentation
- Augmentation de la bande passante

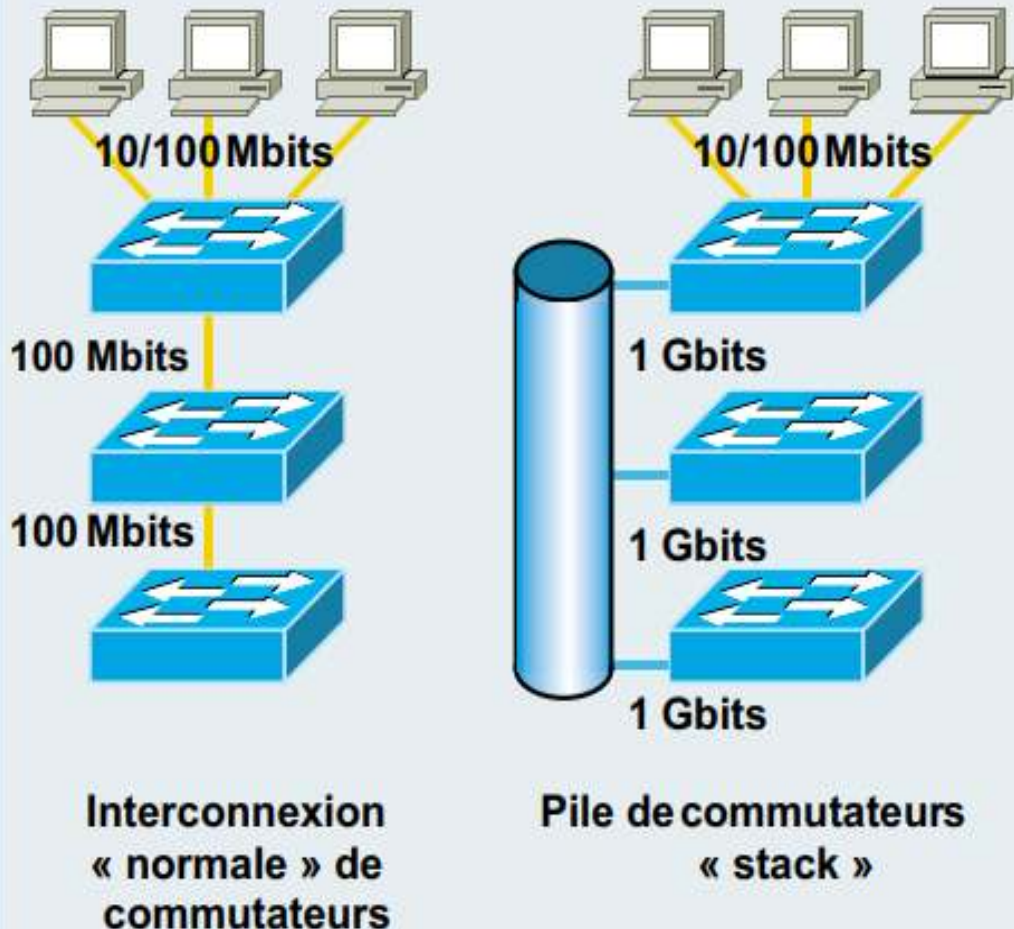
➤ Équipements:

- Bridges
- Switchs
- Routers



Commutation LAN

Densité de ports plus élevée :
Pile de commutateurs

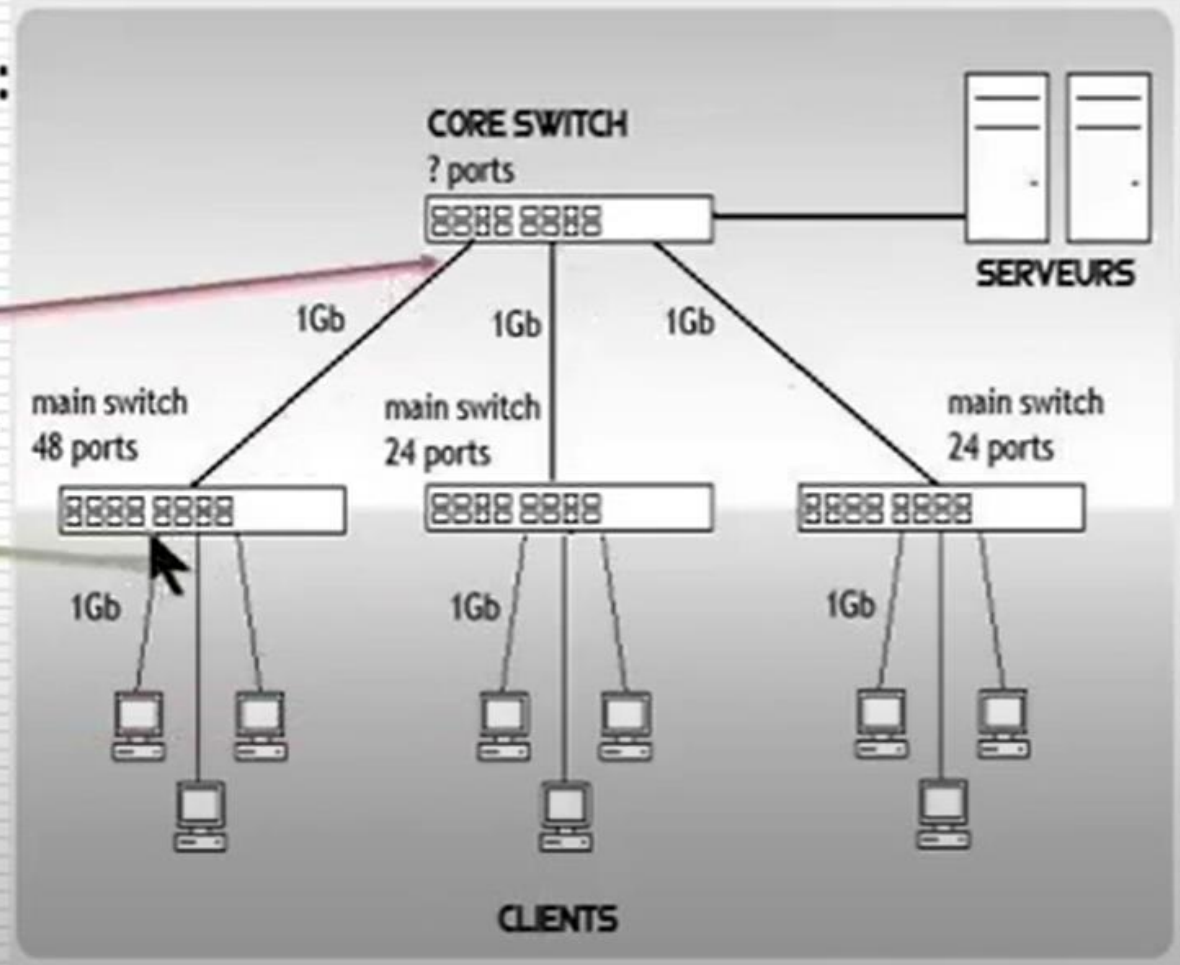


Les commutateurs dits « **stackables** » peuvent être empilés ; c'est-à-dire reliés entre eux par des liens à haut débit (Gigabit), ce qui leur permet d'échanger leurs **données dix fois plus rapidement** que s'ils étaient connectés entre eux par un lien 100 Mbits classique.

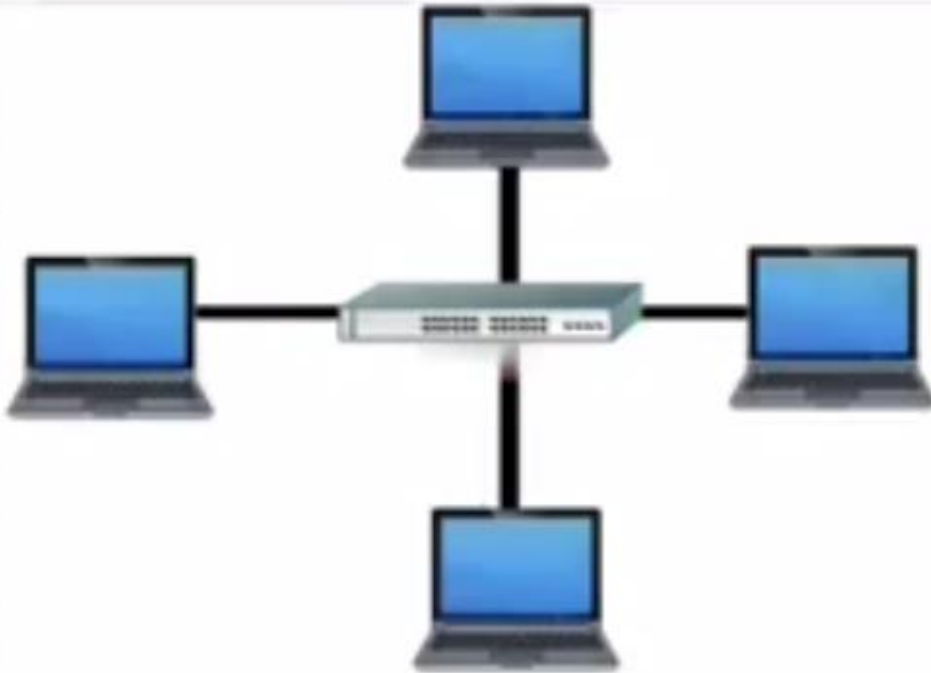
Cette fonctionnalité permet de créer des piles de commutateurs **à forte densité de ports**, jusqu'à 432 ports (9 commutateurs)

Commutation LAN

- Un commutateur fonctionne:
- **Par segment** (plusieurs stations Ethernet par port).
- **Par port** (une seule station Ethernet par port).



Commutation LAN



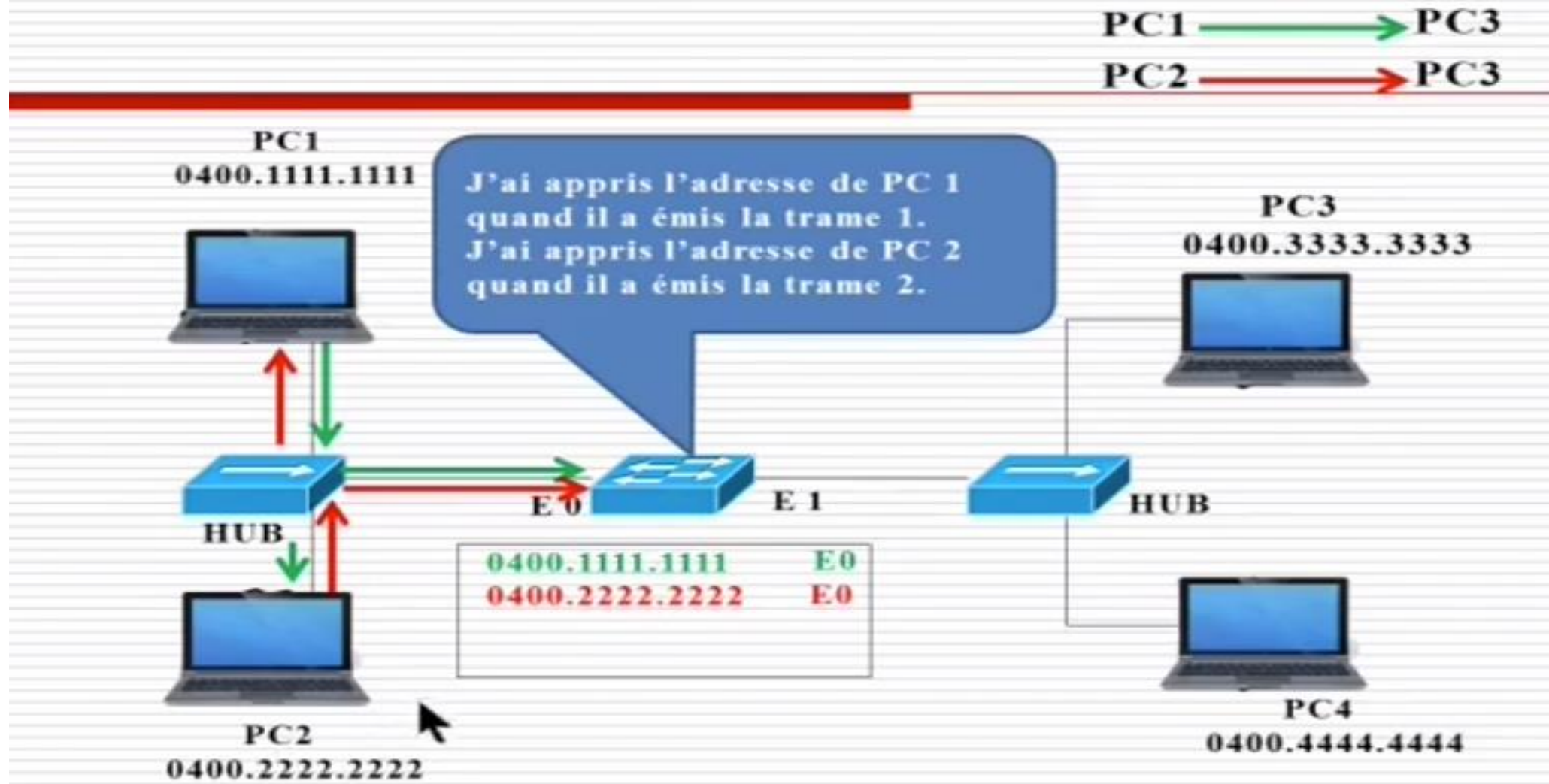
Un commutateur peut mettre simultanément plusieurs ports en relation, sans que le débit de chacun en souffre.

Si une trame est à destination d'un port déjà occupé, le commutateur la **mémorise** pour la délivrer quand le port sera disponible.

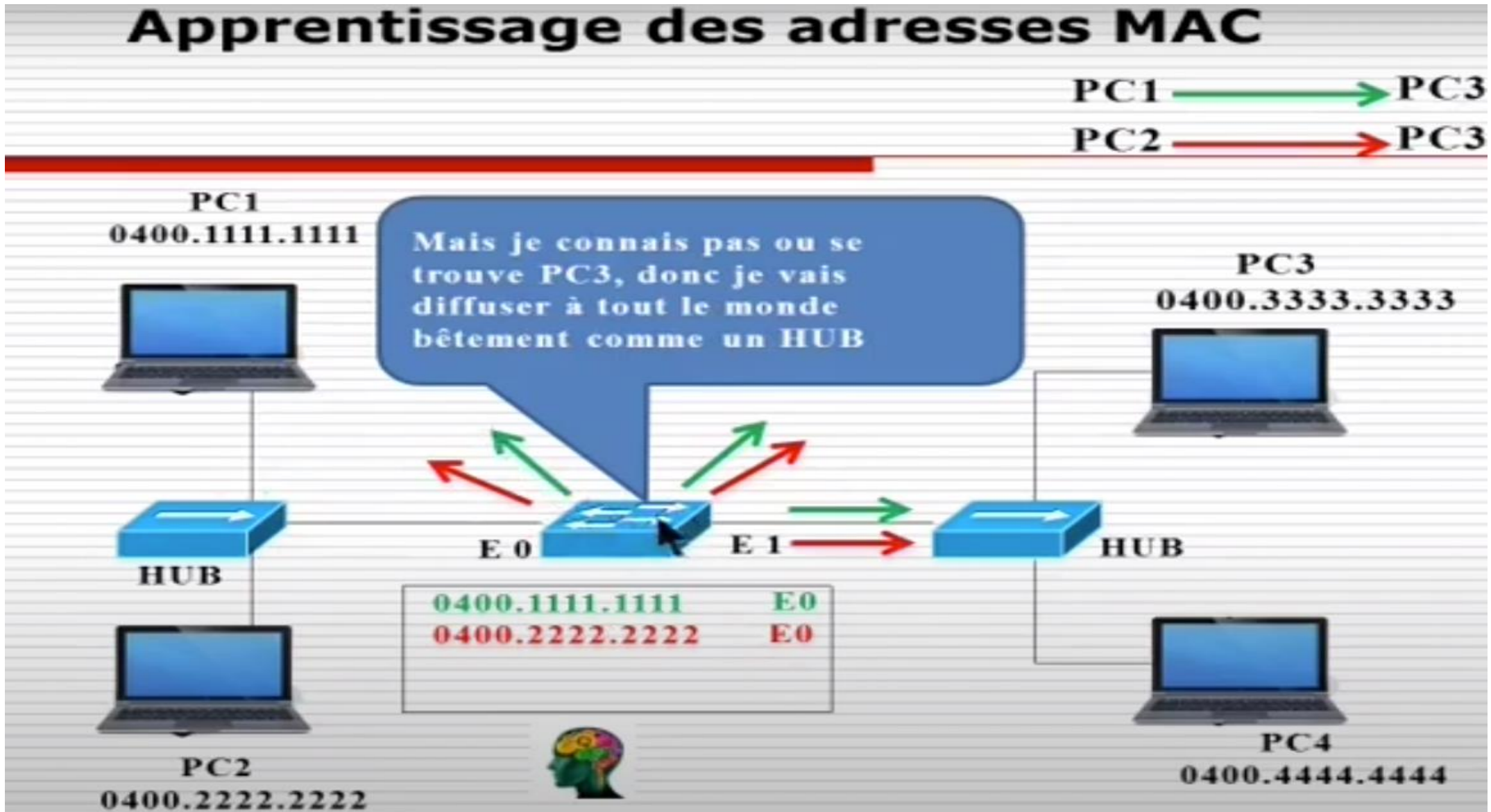


Commutation LAN : fonctions de switch (1)

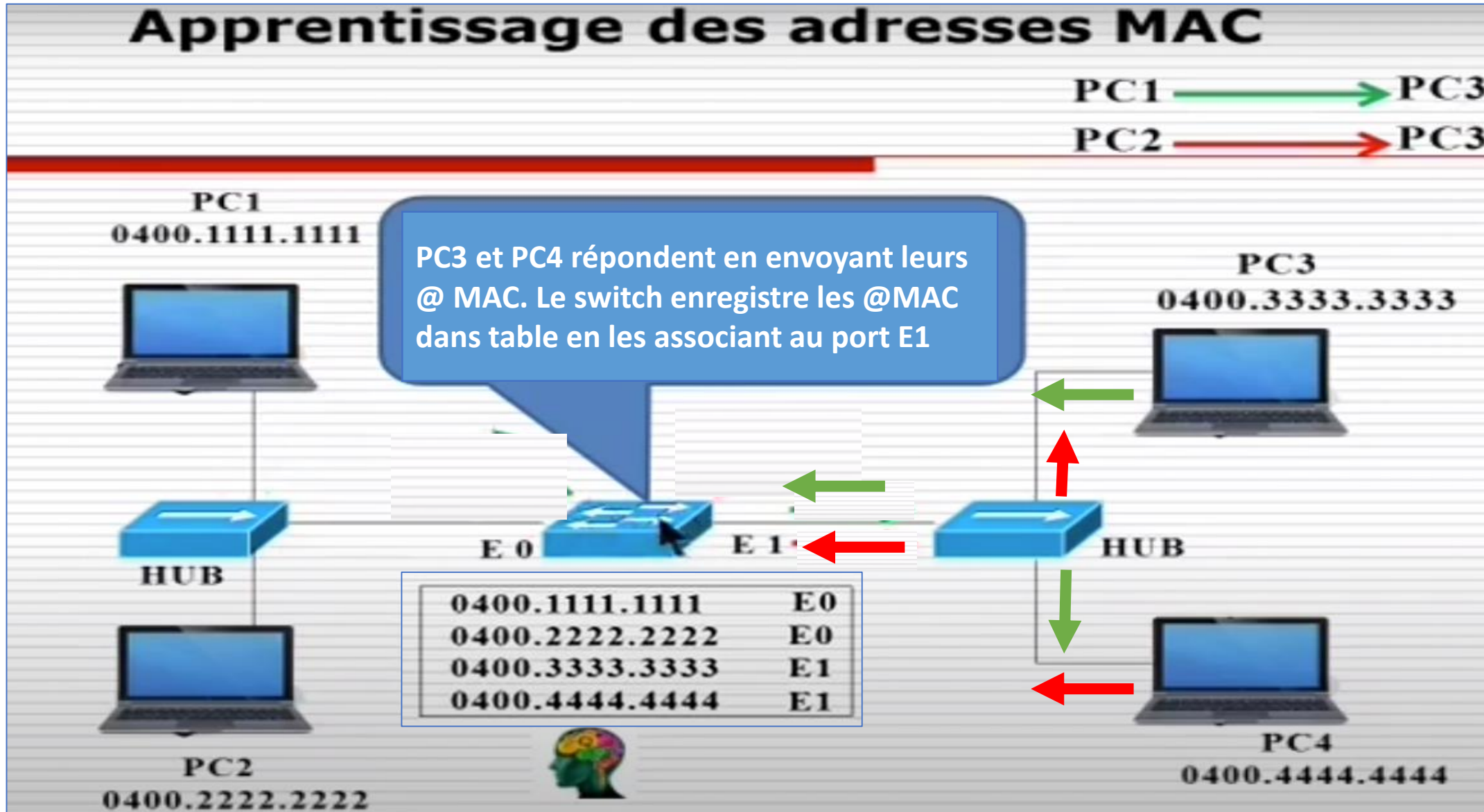
Apprentissage des adresses MAC



Commutation LAN : fonctions de switch (1)



Commutation LAN : fonctions de switch (1)



Commutation LAN : fonctions de switch (2)

Filtrage

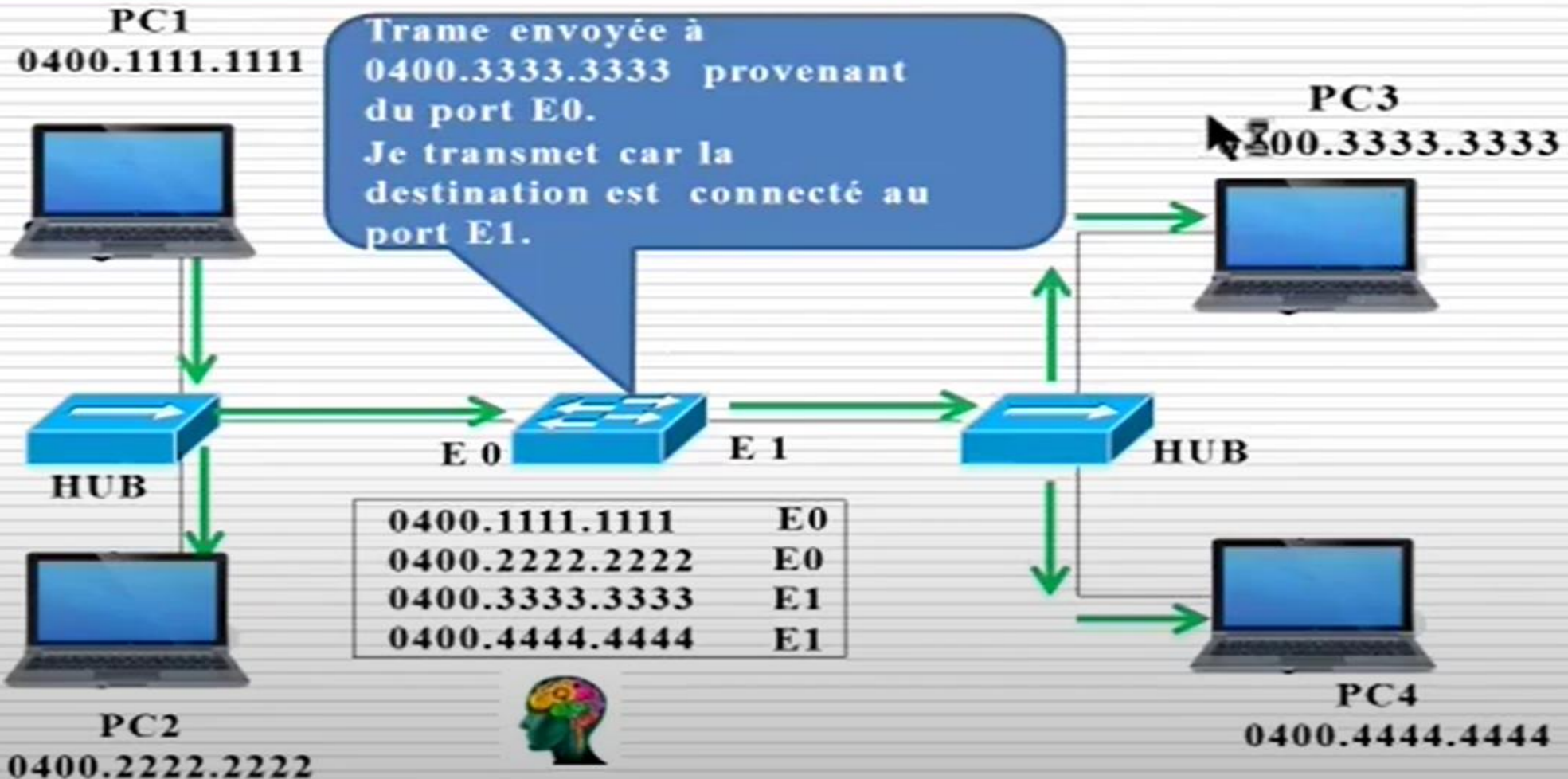
PC1 → PC2



Commutation LAN : fonctions de switch (3)

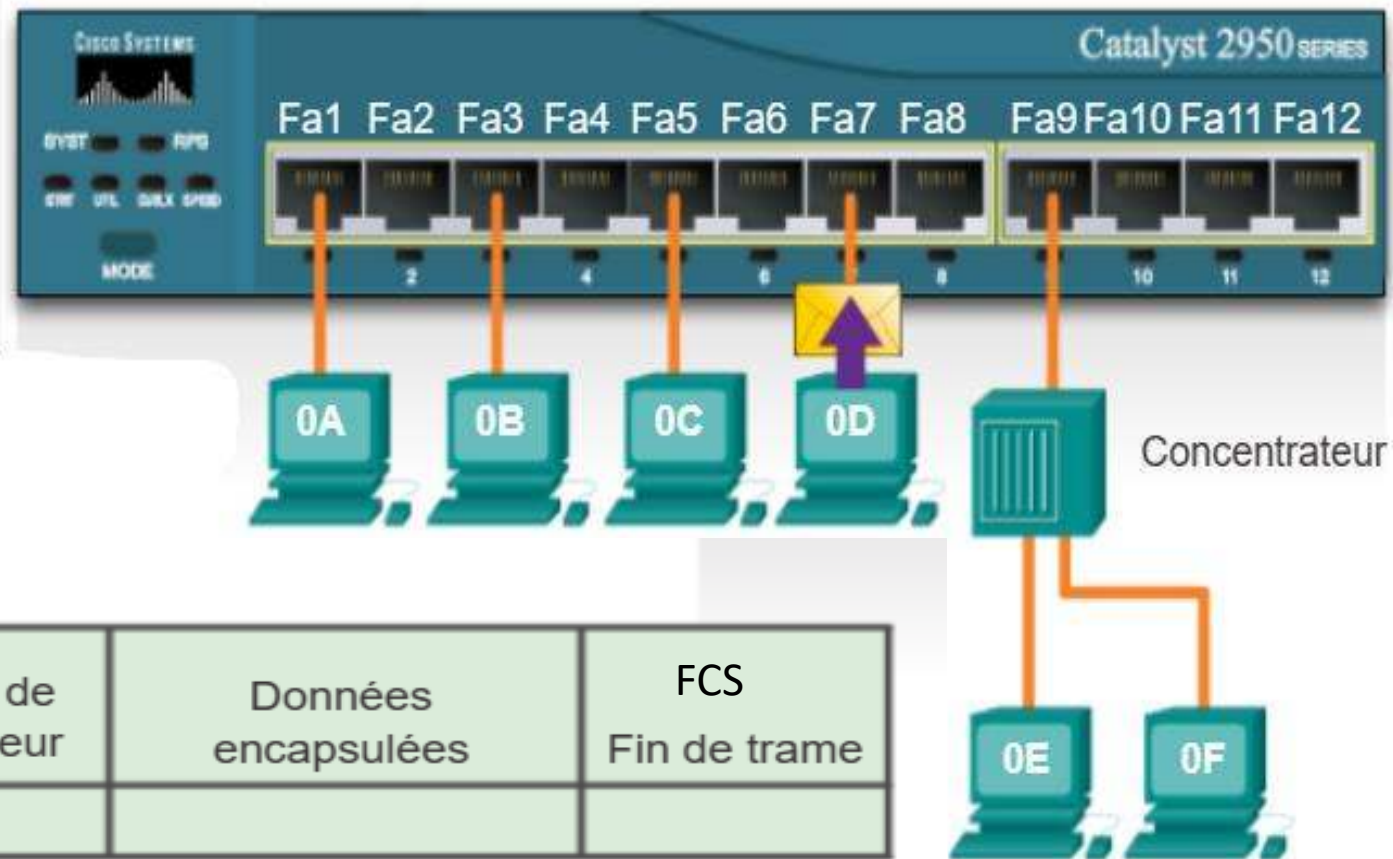
Transmission

PC1 → PC3



Exercice

Déterminer comment le commutateur transfère une trame, compte tenu des adresses MAC source et destination, ainsi que des informations dans la table MAC de commutation



Trame

Préambule	Adresse MAC de destination	Adresse MAC source	Type de longueur	Données encapsulées	FCS Fin de trame
	0B	0D			

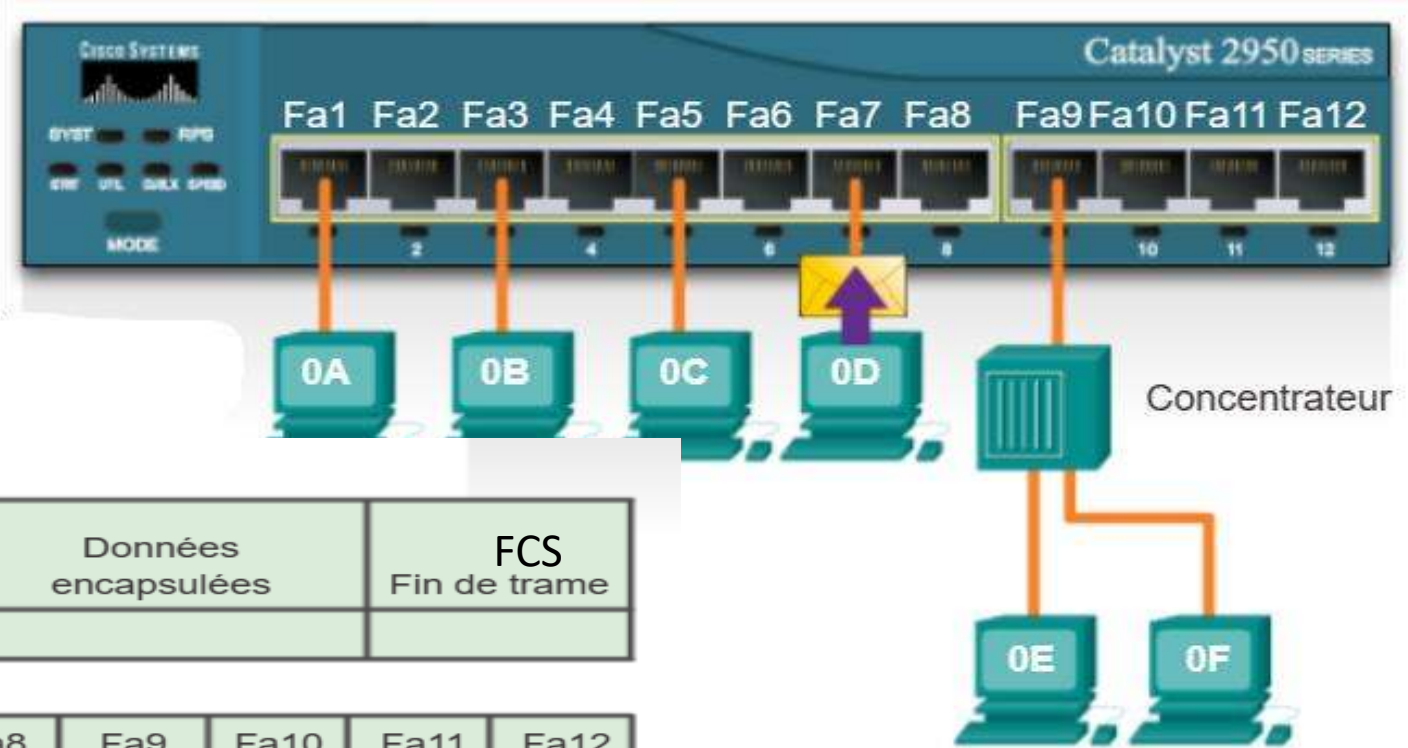
Table MAC

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
								0E			

Question 1 : où le commutateur transmet-il la trame ?

- ☐ Fa1 ☐ Fa2 ☐ Fa3 ☐ Fa4 ☐ Fa5 ☐ Fa6 ☐ Fa7 ☐ Fa8 ☐ Fa9 ☐ Fa10 ☐ Fa11 ☐ Fa12

Exercice



Trame

Préambule	Adresse MAC de destination	Adresse MAC source	Type de longueur	Données encapsulées	FCS Fin de trame
	0B	0D			

Table MAC

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
								0E			

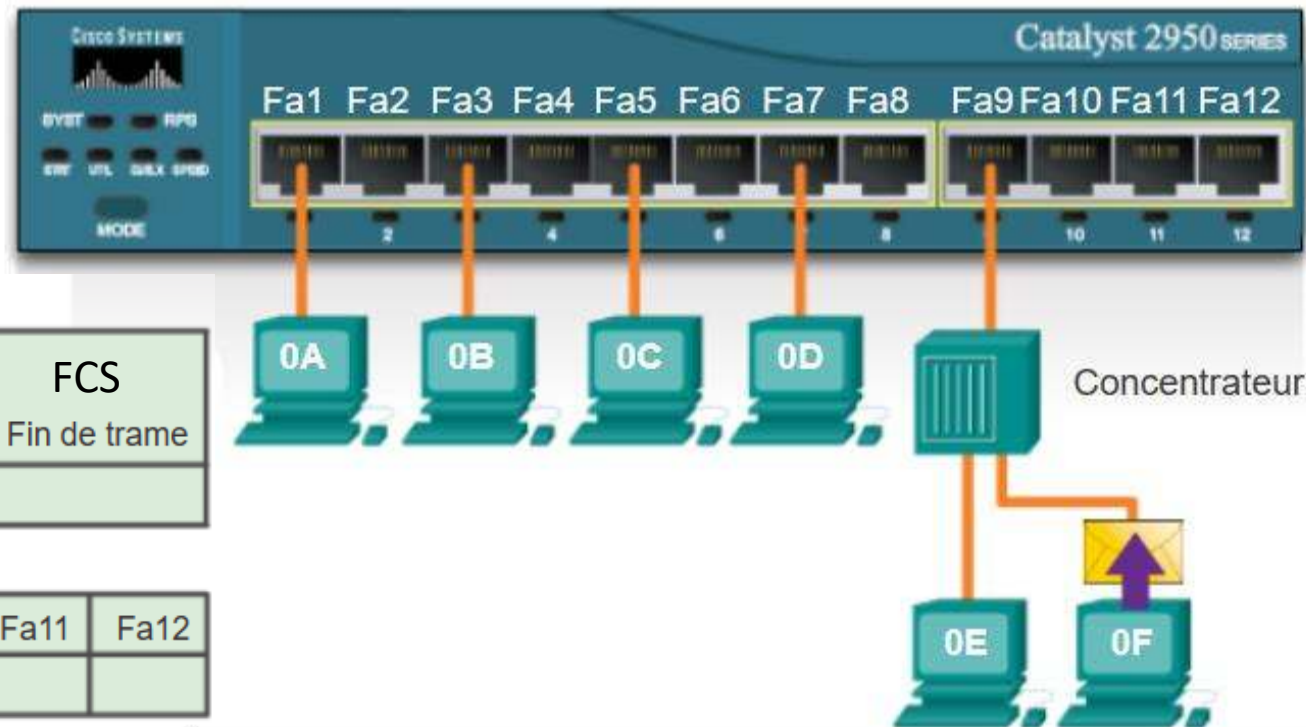
Question 1 : où le commutateur transmet-il la trame ?

- ☒ Fa1
 ☐ Fa2
 ☒ Fa3
 ☐ Fa4
 ☒ Fa5
 ☐ Fa6
 ☐ Fa7
 ☐ Fa8
 ☒ Fa9
 ☐ Fa10
 ☐ Fa11
 ☐ Fa12

Question 2 : lorsque le commutateur transmet la trame, quels énoncés sont vrais ?

- ☒ Le commutateur ajoute l'adresse MAC source dans la table MAC.
☐ La trame est une trame de diffusion ; elle est transférée à tous les ports.
☐ La trame est une trame de monodiffusion ; elle est envoyée à un seul port désigné.
☒ La trame est une trame de monodiffusion ; elle inonde tous les ports.
☐ La trame est une trame de monodiffusion, mais elle est abandonnée au niveau du commutateur.

Exercice



Trame

Préambule	Adresse MAC de destination	Adresse MAC source	Type de longueur	Données encapsulées	FCS Fin de trame
	0C	0F			

Table MAC

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
0A		0B						0E			

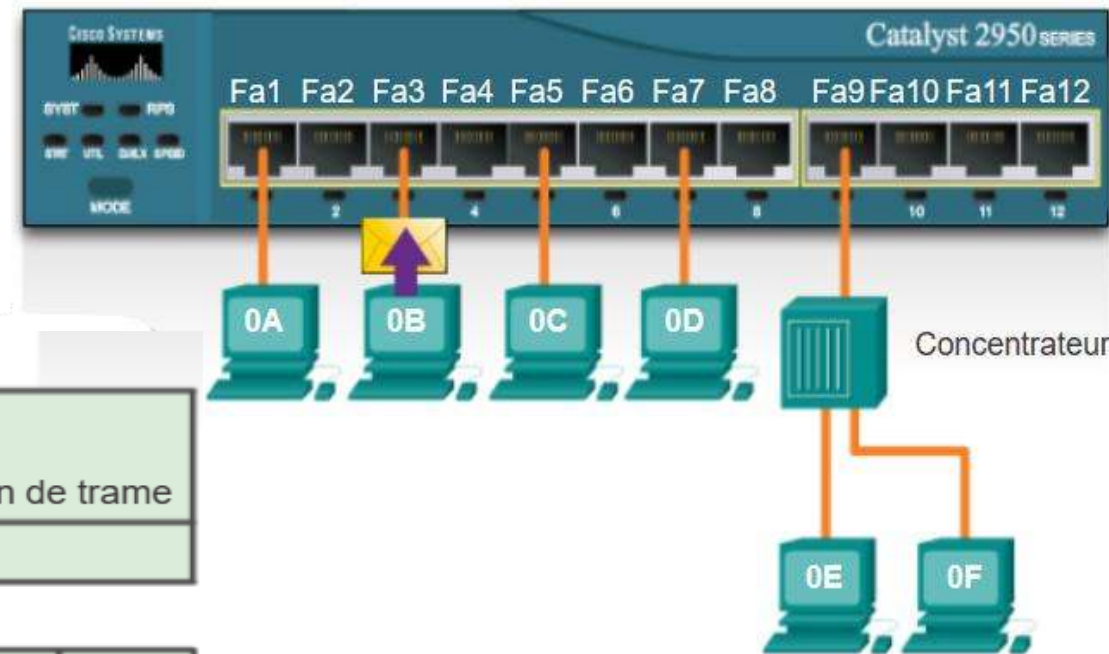
Question 1 : où le commutateur transmet-il la trame ?

- ☒ Fa1
 ☐ Fa2
 ☒ Fa3
 ☐ Fa4
 ☒ Fa5
 ☐ Fa6
 ☒ Fa7
 ☐ Fa8
 ☐ Fa9
 ☐ Fa10
 ☐ Fa11
 ☐ Fa12

Question 2 : lorsque le commutateur transmet la trame, quels énoncés sont vrais ?

- ☒ Le commutateur ajoute l'adresse MAC source dans la table MAC.
☐ La trame est une trame de diffusion ; elle est transférée à tous les ports.
☐ La trame est une trame de monodiffusion ; elle est envoyée à un seul port désigné.
☒ La trame est une trame de monodiffusion ; elle inonde tous les ports.
☐ La trame est une trame de monodiffusion, mais elle est abandonnée au niveau du commutateur.

Exercice



Trame

Préambule	Adresse MAC de destination	Adresse MAC source	Type de longueur	Données encapsulées	Fin de trame
	0C	0B			

Table MAC

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
0A		0B				0D		0E 0F			

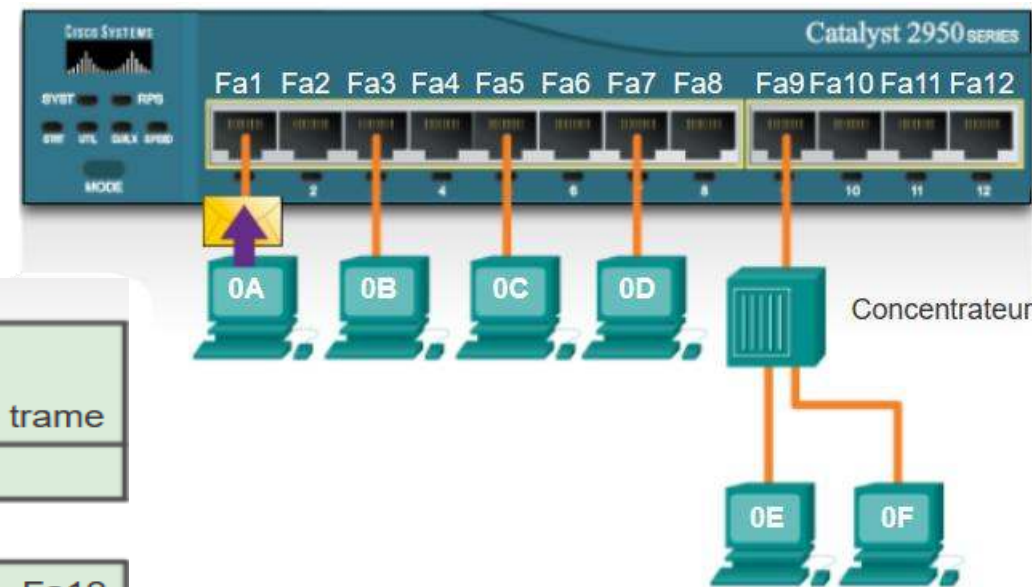
Question 1 : où le commutateur transmet-il la trame ?

- ☒ Fa1 ☐ Fa2 ☐ Fa3 ☐ Fa4 ☒ Fa5 ☐ Fa6 ☒ Fa7 ☐ Fa8 ☒ Fa9 ☐ Fa10 ☐ Fa11 ☐ Fa12

Question 2 : lorsque le commutateur transmet la trame, quels énoncés sont vrais ?

- ☐ Le commutateur ajoute l'adresse MAC source dans la table MAC.
- ☐ La trame est une trame de diffusion ; elle est transférée à tous les ports.
- ☐ La trame est une trame de monodiffusion ; elle est envoyée à un seul port désigné.
- ☒ La trame est une trame de monodiffusion ; elle inonde tous les ports.
- ☐ La trame est une trame de monodiffusion, mais elle est abandonnée au niveau du commutateur.

Exercice



Trame

Préambule	Adresse MAC de destination	Adresse MAC source	Type de longueur	Données encapsulées	Fin de trame
	0B	0A			

Table MAC

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
0A		0B		0C		0D		0E			

Question 1 : où le commutateur transmet-il la trame ?

- ☐ Fa1 ☐ Fa2 ☒ Fa3 ☐ Fa4 ☐ Fa5 ☐ Fa6 ☐ Fa7 ☐ Fa8 ☐ Fa9 ☐ Fa10 ☐ Fa11 ☐ Fa12

Question 2 : lorsque le commutateur transmet la trame, quels énoncés sont vrais ?

- ☐ Le commutateur ajoute l'adresse MAC source dans la table MAC.
- ☐ La trame est une trame de diffusion ; elle est transférée à tous les ports.
- ☒ La trame est une trame de monodiffusion ; elle est envoyée à un seul port désigné.
- ☐ La trame est une trame de monodiffusion ; elle inonde tous les ports.
- ☐ La trame est une trame de monodiffusion, mais elle est abandonnée au niveau du commutateur.

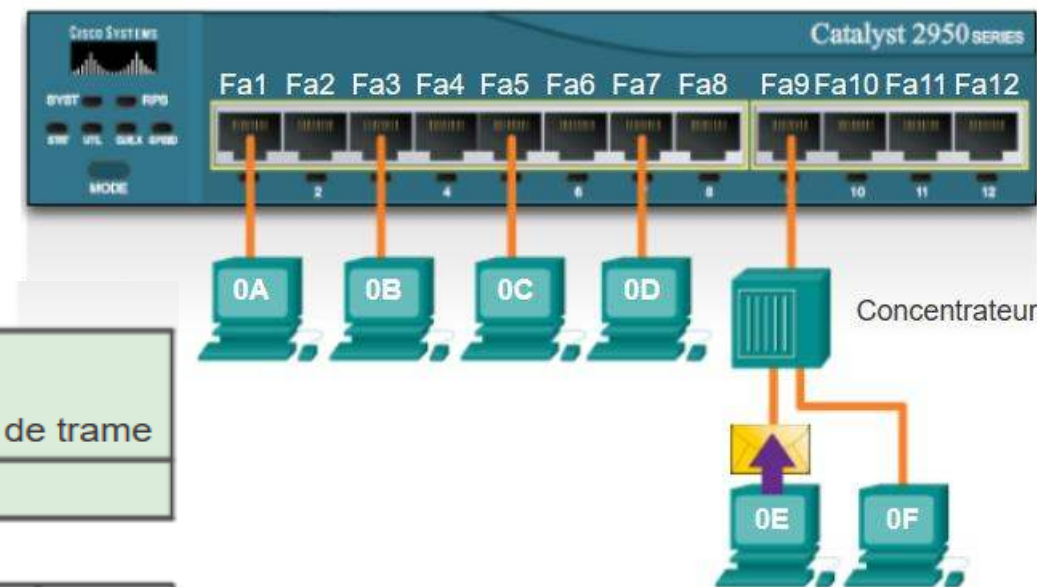
Exercice

Trame

Préambule	Adresse MAC de destination	Adresse MAC source	Type de longueur	Données encapsulées	Fin de trame
	0A	0E			

Table MAC

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
0A						0D		0E			



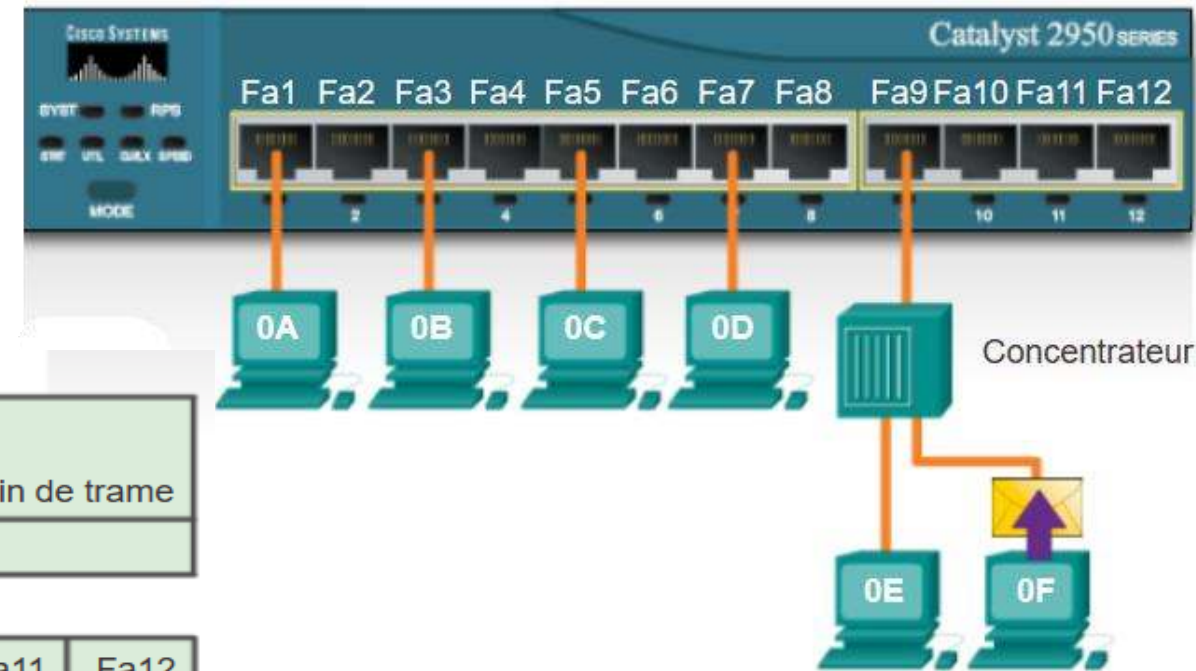
Question 1 : où le commutateur transmet-il la trame ?

- ☒ Fa1 ☐ Fa2 ☐ Fa3 ☐ Fa4 ☐ Fa5 ☐ Fa6 ☐ Fa7 ☐ Fa8 ☐ Fa9 ☐ Fa10 ☐ Fa11 ☐ Fa12

Question 2 : lorsque le commutateur transmet la trame, quels énoncés sont vrais ?

- ☐ Le commutateur ajoute l'adresse MAC source dans la table MAC.
- ☐ La trame est une trame de diffusion ; elle est transférée à tous les ports.
- ☒ La trame est une trame de monodiffusion ; elle est envoyée à un seul port désigné.
- ☐ La trame est une trame de monodiffusion ; elle inonde tous les ports.
- ☐ La trame est une trame de monodiffusion, mais elle est abandonnée au niveau du commutateur.

Exercice



Trame

Préambule	Adresse MAC de destination	Adresse MAC source	Type de longueur	Données encapsulées	Fin de trame
	FF	0F			

Table MAC

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
0A		0B		0C				0F			

Question 1 : où le commutateur transmet-il la trame ?

- ☒ Fa1 ☐ Fa2 ☒ Fa3 ☐ Fa4 ☒ Fa5 ☐ Fa6 ☒ Fa7 ☐ Fa8 ☐ Fa9 ☐ Fa10 ☐ Fa11 ☐ Fa12

Question 2 : lorsque le commutateur transmet la trame, quels énoncés sont vrais ?

- ☐ Le commutateur ajoute l'adresse MAC source dans la table MAC.
- ☒ La trame est une trame de diffusion, elle est transférée à tous les ports.
- ☐ La trame est une trame de monodiffusion ; elle est envoyée à un seul port désigné.
- ☐ La trame est une trame de monodiffusion ; elle inonde tous les ports.
- ☐ La trame est une trame de monodiffusion, mais elle est abandonnée au niveau du commutateur.

Rôles de commutateurs

- **La commutation de trames de données :**

Se produit lorsqu'une trame qui parvenue au média d'entrée est transmise au média de sortie

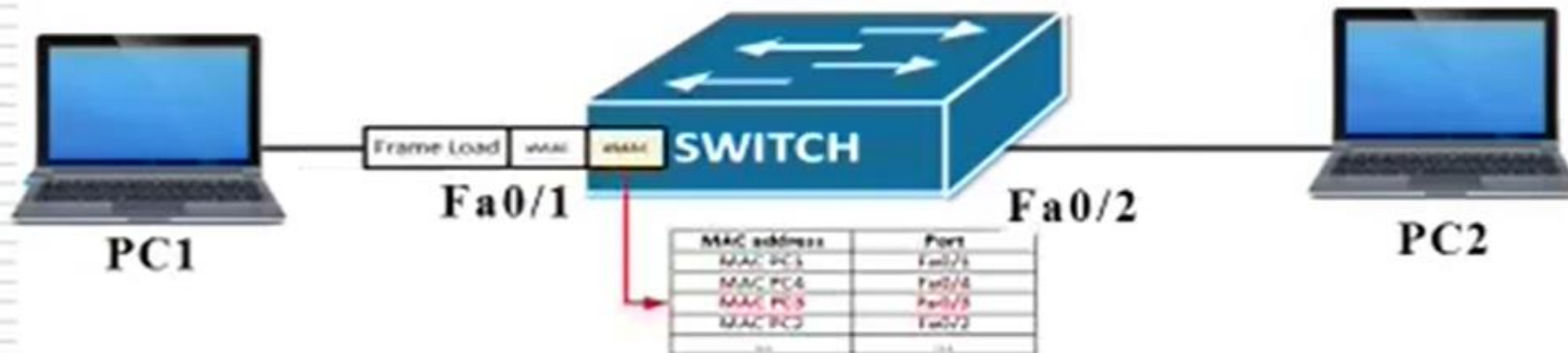
- **La gestion des opérations de commutation:**

Création et la gestion des table de commutation

Modes de transfert

Cut through - mode direct:

1. Le commutateur LAN peut lire l'adresse MAC dès qu'un paquet est détecté.
2. Après avoir stocké les 6 octets (l'adresse MAC), le paquet est envoyé immédiatement à la destination, alors même que le reste du paquet arrive dans le commutateur.



Modes de transfert

Store and forward –

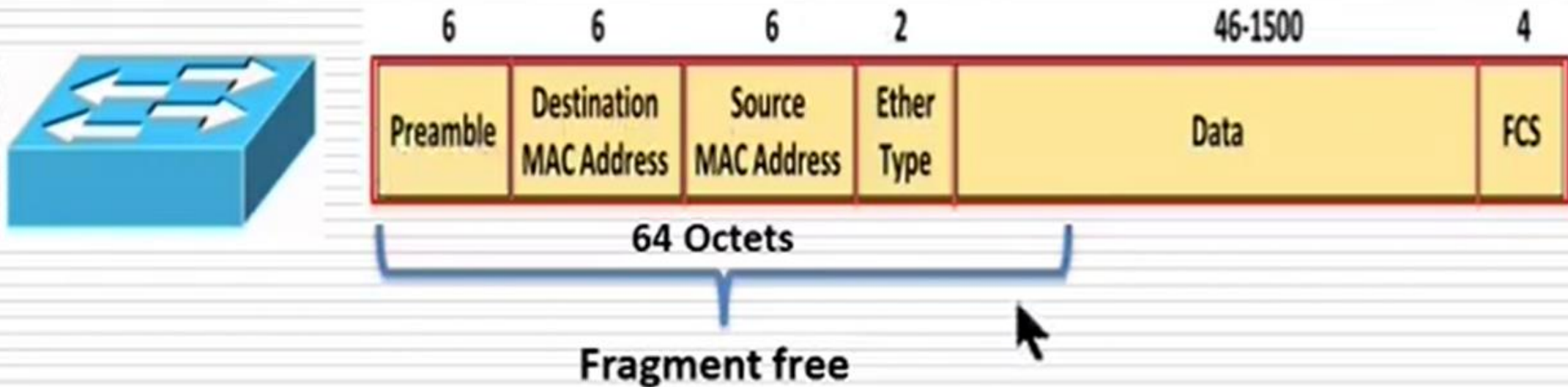
1. Enregistre le paquet entier dans la mémoire cache et vérifie s'il y a des erreurs
2. Si le paquet a une erreur, il sera rejeté.
3. Sinon, le commutateur lira l'adresse MAC et enverra le paquet au destinataire.



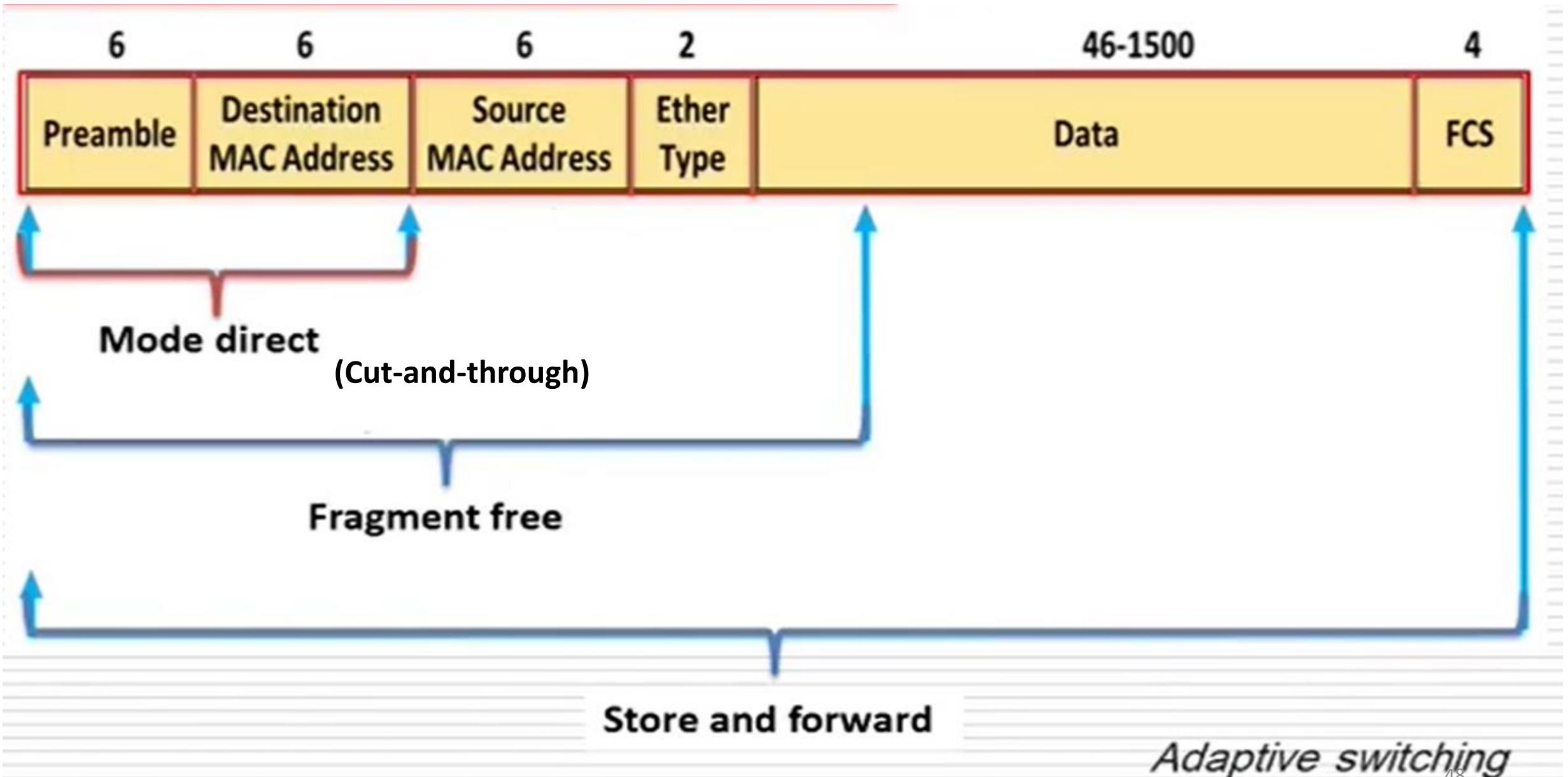
Modes de transfert

Fragment free - moins courante

1. Fonctionne de la même manière que le “cut through”, sauf que les **64 premiers octets** du paquet sont stockés avant d'être envoyé.
2. **Pourquoi?** la plupart des erreurs, et toutes les collisions, se produisent pendant les premiers 64 octets d'un paquet.



Modes de transfert



Sélectionner le mode adéquat selon la condition du réseau

Commutation LAN

- La commutation comme concept général
 - Un commutateur prend une décision en fonction du **port d'entrée** et **de destination**
 - Un commutateur LAN gère une **table** qu'il utilise pour déterminer comment acheminer le trafic
 - Les commutateurs LAN Cisco transmettent des **trames Ethernet** basées sur **l'adresse MAC de destination** des trames.

Commutation LAN

- Remplissage dynamique de la table d'adresses MAC
 - Un commutateur doit d'abord savoir quels équipements figurent sur chaque port avant de pouvoir transmettre une trame
 - Il crée une table appelée table d'adresses MAC, ou table de mémoire associative (**CAM : Content-Addressable Memory**)
 - Le port <-> de mappage de périphériques est stocké dans la table CAM
 - La CAM est un type particulier de mémoire utilisé dans des applications de recherche haut débit.
 - Lorsqu'un commutateur reçoit une trame entrante dont l'adresse MAC ne figure pas dans la table CAM, il l'envoie à tous les ports, sauf à celui qui l'a reçue.

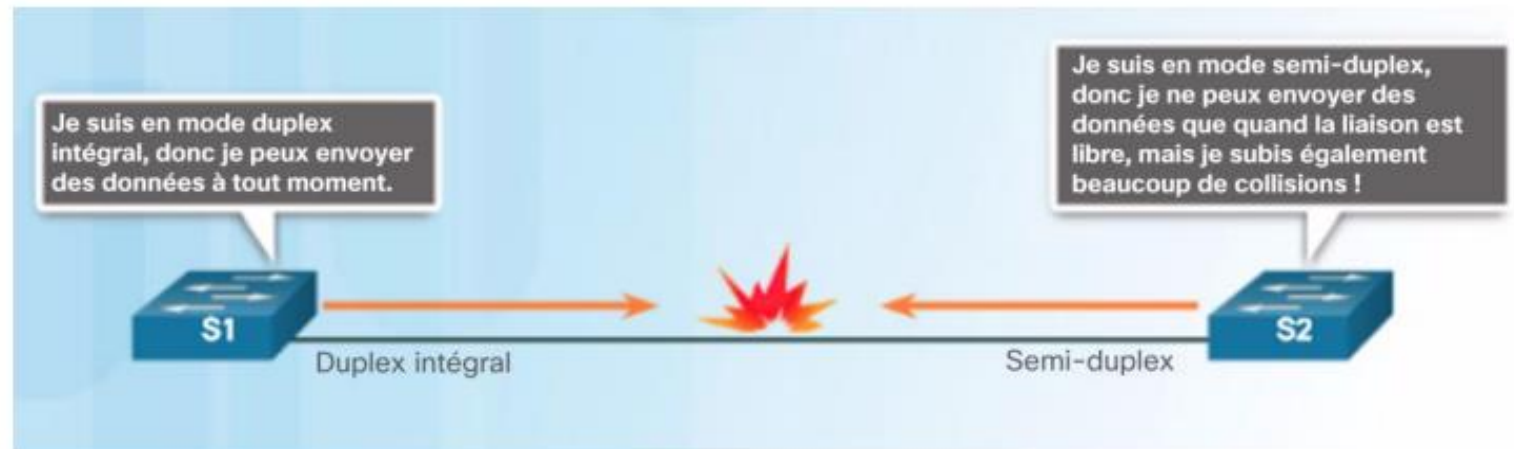
Commutation LAN

- Le domaine de collision est le segment sur lequel **les périphériques sont en concurrence** les uns avec les autres pour communiquer
- Tous les ports d'un **concentrateur** appartiennent au **même domaine de collision**
- Chaque **port** d'un **commutateur** constitue un **domaine de collision**
- Le commutateur décompose le segment en domaines de collision plus petits, ce qui facilite les choses pour les périphériques.

Commutation LAN

Paramètres du mode duplex et de vitesse

- Deux types de paramètres bidirectionnels sont employés pour les communications dans un réseau Ethernet :
 - **Mode duplex intégral** : les deux extrémités de la connexion peuvent envoyer et recevoir des données simultanément.
 - **Mode semi-duplex** : une seule extrémité de la connexion peut envoyer des données à la fois.
- La plupart des périphériques utilisent la négociation automatique qui permet à deux périphériques d'échanger automatiquement des informations sur le débit et les fonctionnalités duplex et de choisir le mode le plus performant.
- Le **conflit de mode duplex** est une cause fréquente de problèmes de performance avec les liaisons Ethernet. Il se produit lorsqu'un port sur la liaison fonctionne en semi-duplex tandis que l'autre port fonctionne en mode duplex intégral.



Commutation LAN

- Le domaine de diffusion représente l'**étendue** du réseau dans laquelle une trame de diffusion peut être « entendue ».
- Les commutateurs envoient les trames de diffusion à **tous les ports**. C'est pourquoi ils ne segmentent pas les domaines de diffusion.
- Tous les ports d'un commutateur (avec la configuration par défaut) appartiennent au même domaine de diffusion
- Si deux commutateurs ou plus sont connectés, les diffusions sont envoyées vers **tous les ports de tous les commutateurs** (à l'exception de celui qui les a initialement reçues)

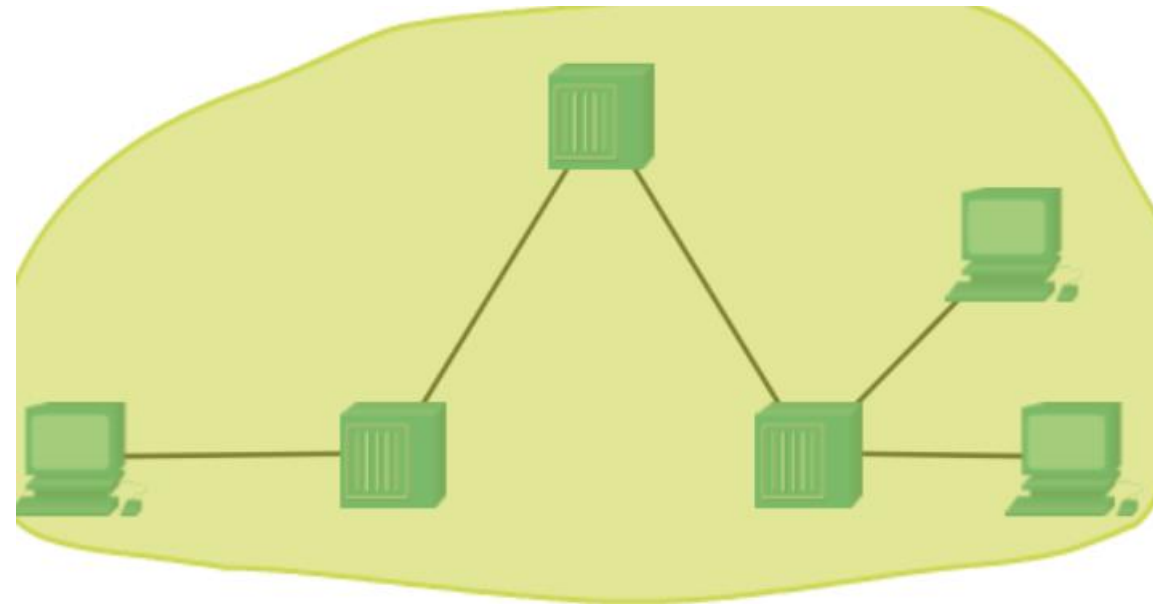
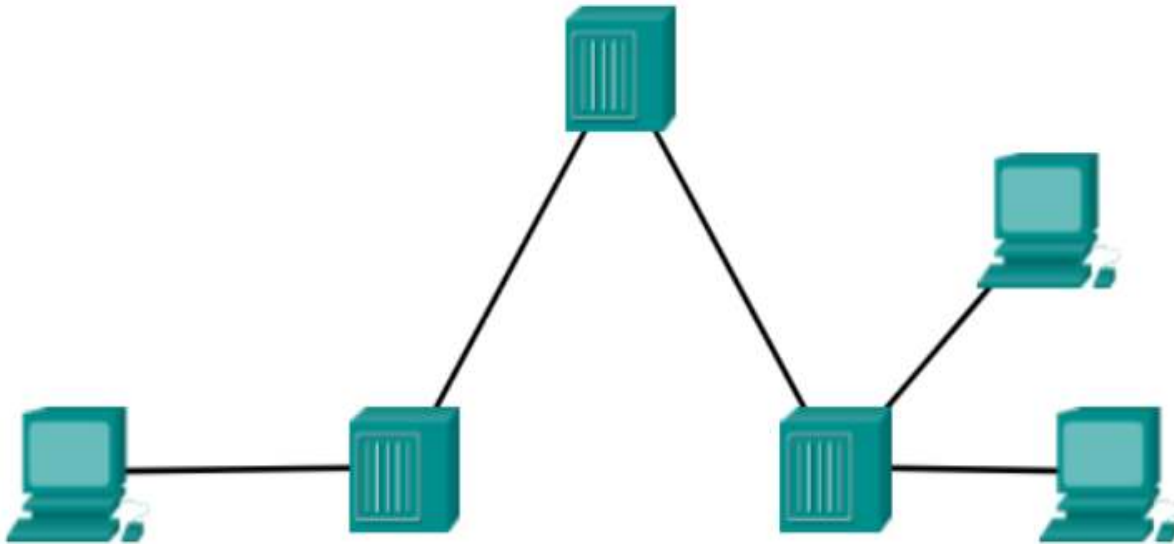
Réduction de l'encombrement du réseau

Les commutateurs contribuent à réduire l'encombrement du réseau :

- Ils facilitent la segmentation d'un LAN en domaines de collision séparés
- Ils assurent une communication bidirectionnelle simultanée entre les périphériques
- Ils tirent profit de leur densité de ports la plus élevée
- Ils mettent les trames volumineuses dans la mémoire tampon
- Ils utilisent les ports haut débit
- Ils exploitent leur méthode rapide de commutation interne
- Ils représentent un faible coût par port

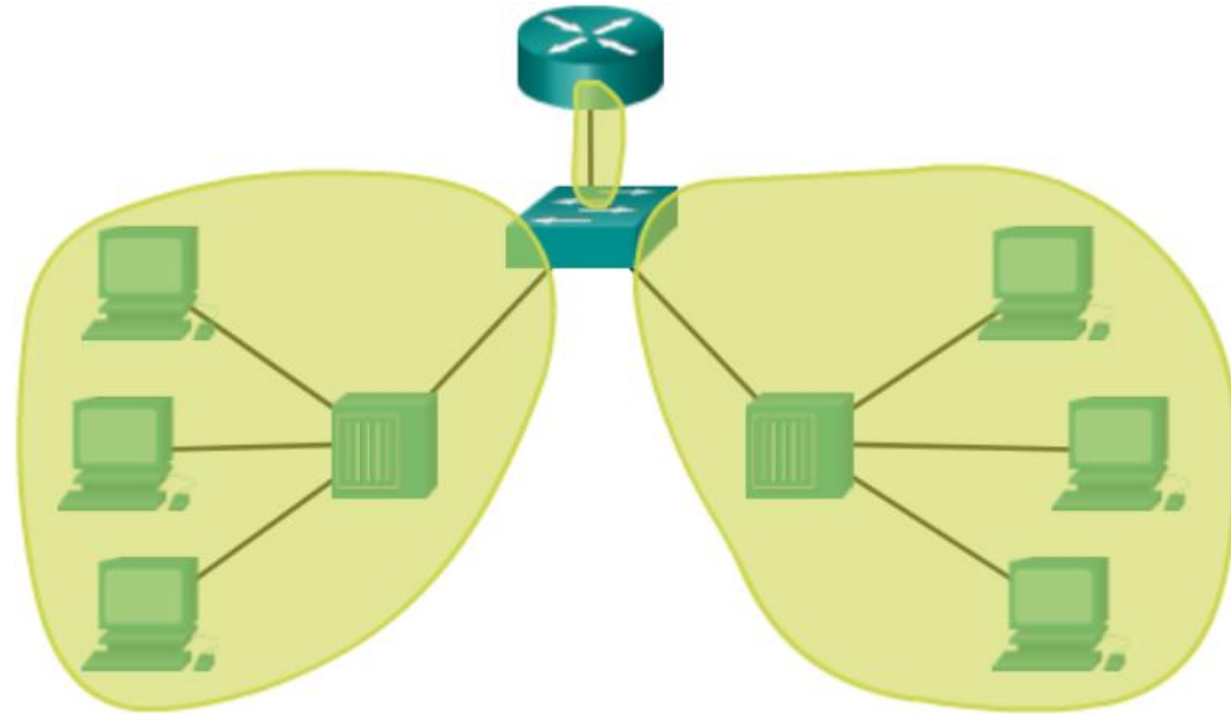
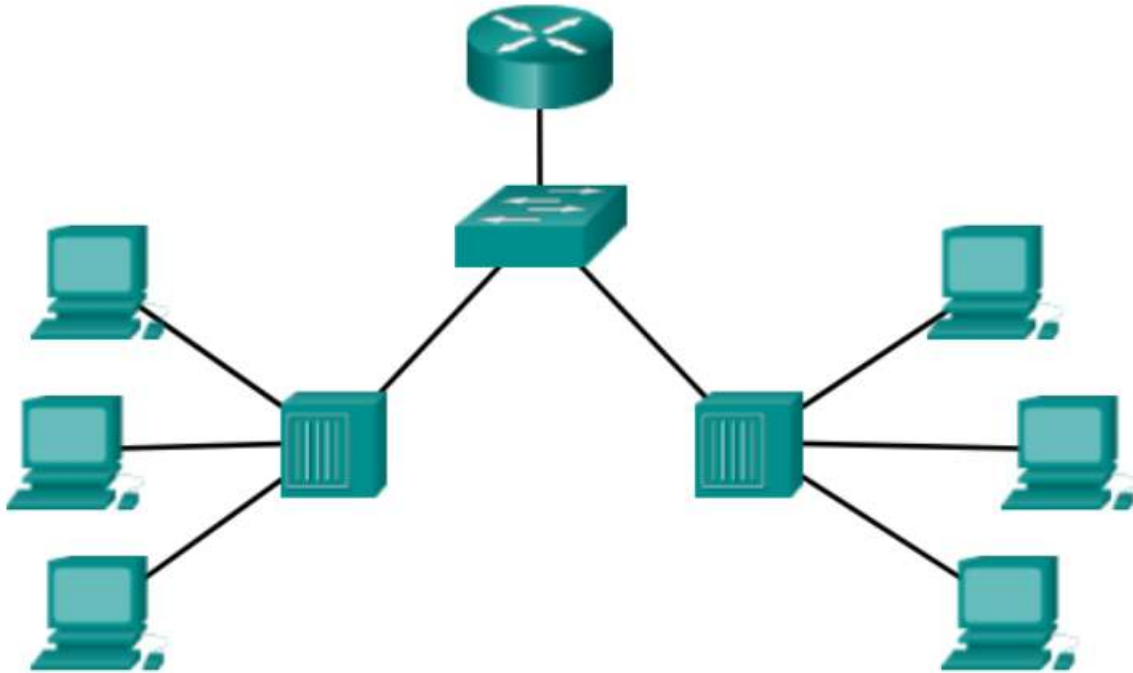
Exercice

Représenter les domaines de collision



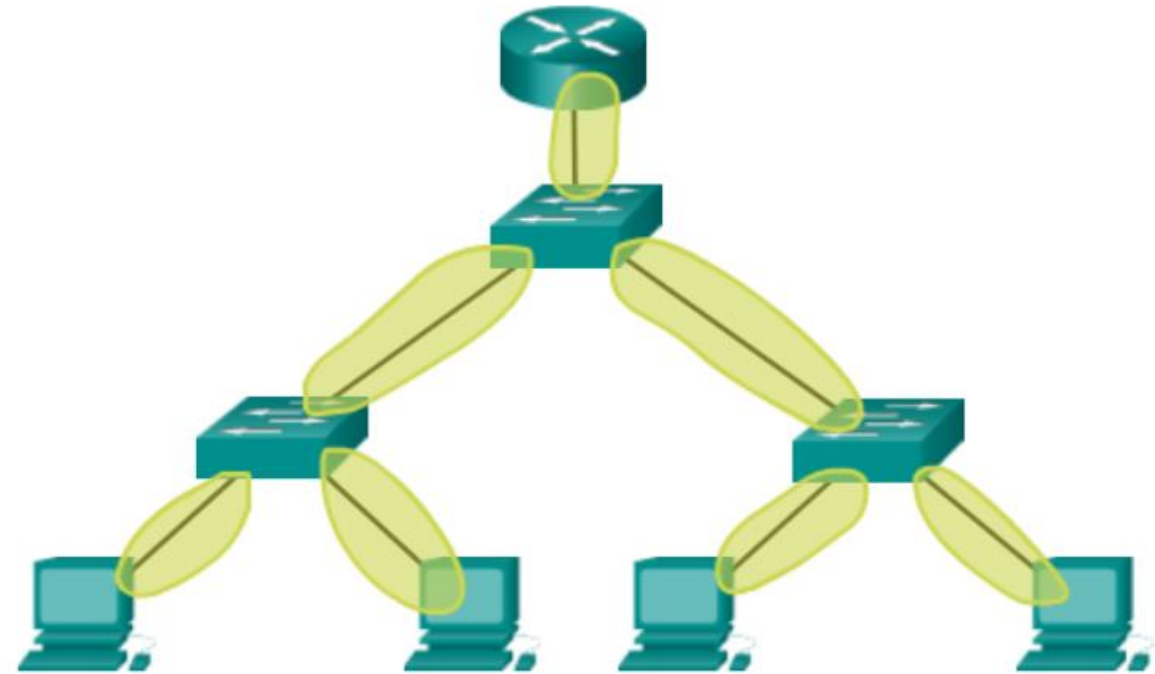
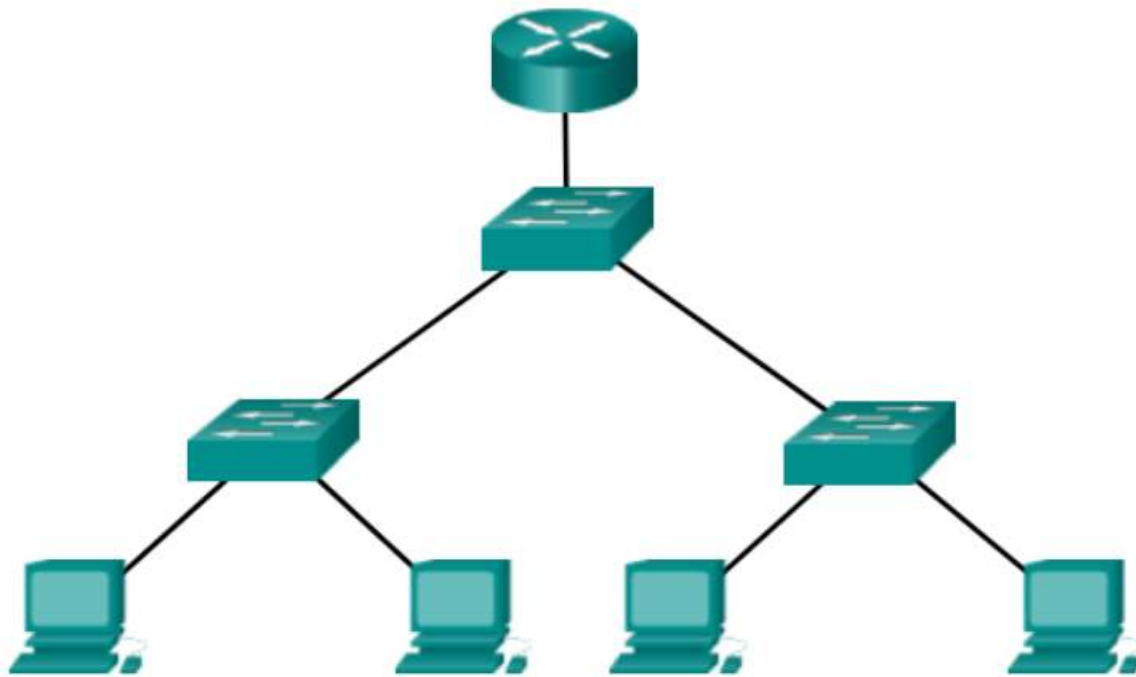
Exercice

Représenter les domaines de collision



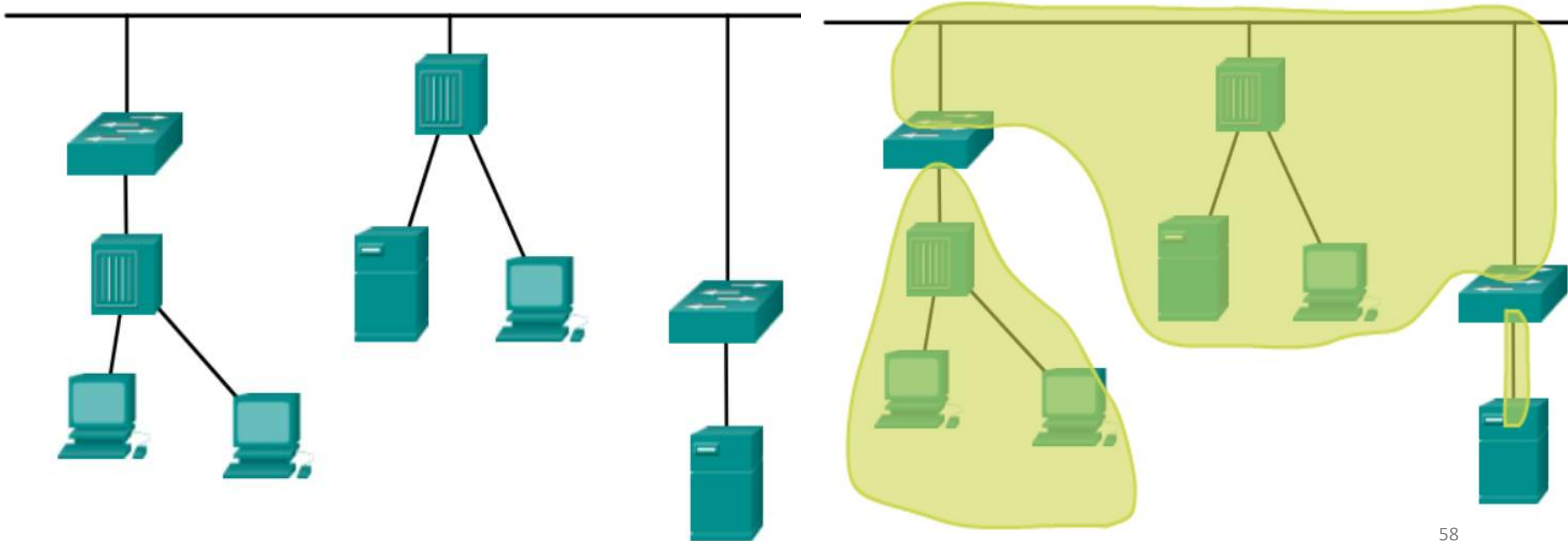
Exercice

Représenter les domaines de collision



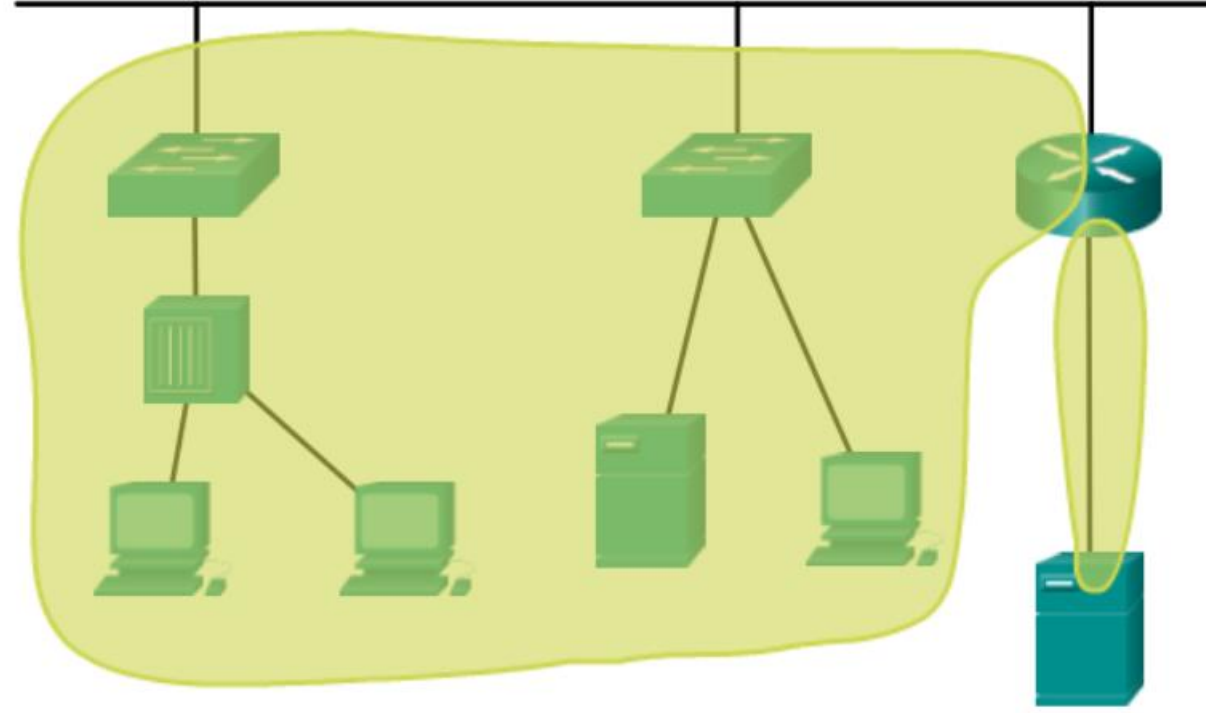
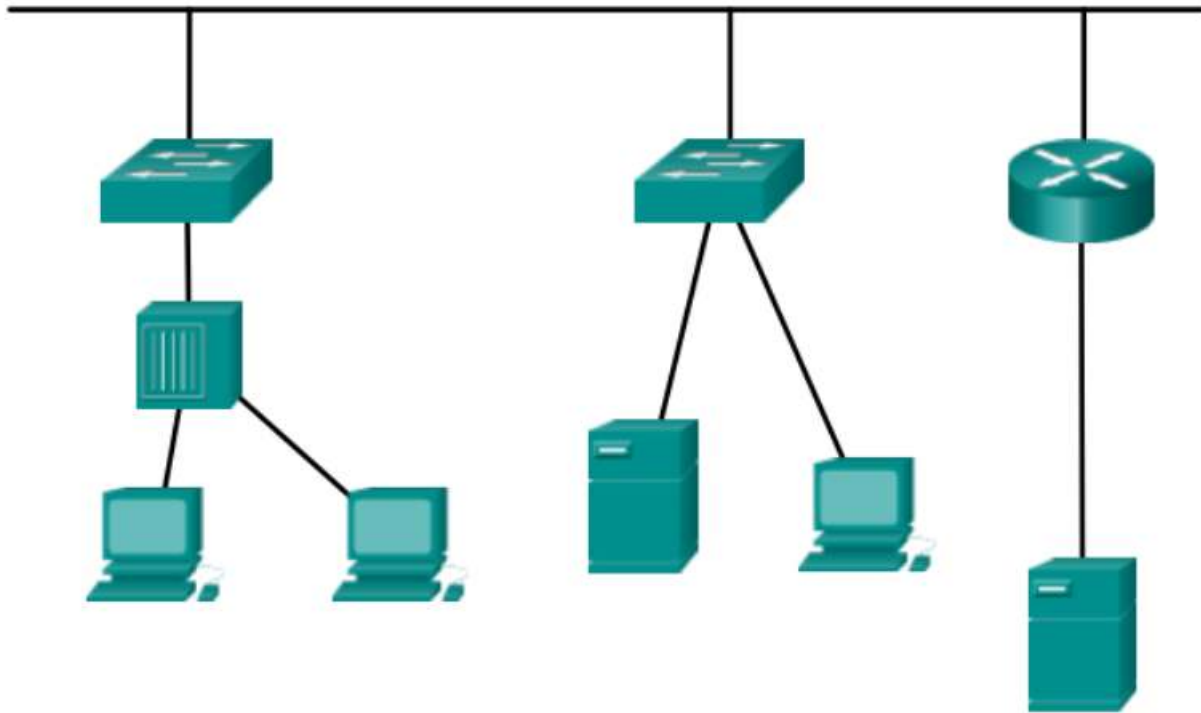
Exercice

Représenter les domaines de collision



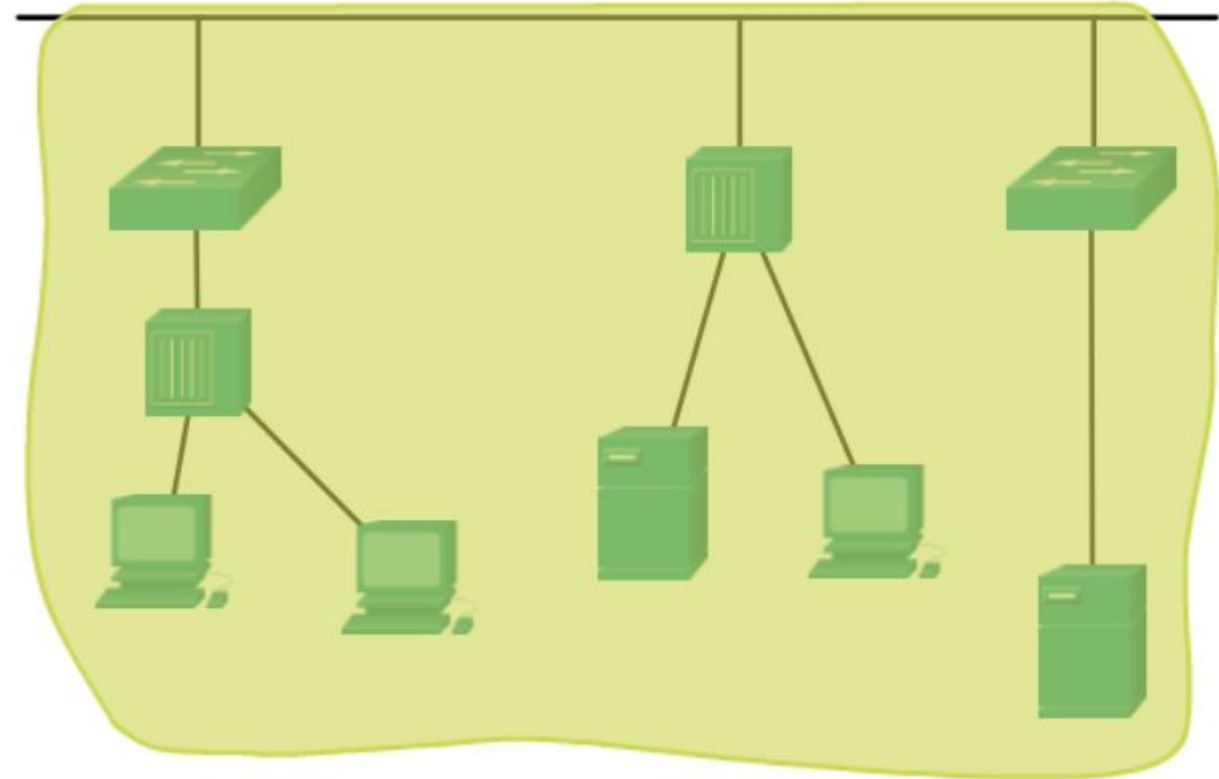
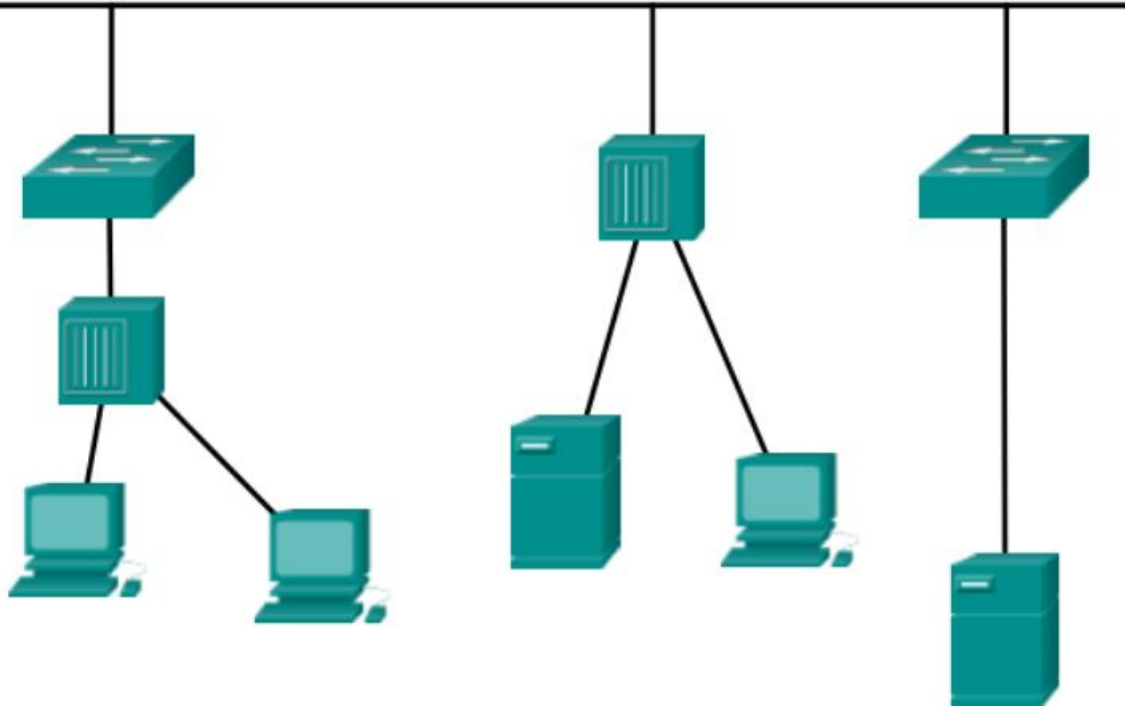
Exercice

Représenter les domaines de diffusion



Exercice

Représenter les domaines de diffusion



Risques de sécurité

➤ **ARP spoofing** : trompe l'ordinateur ciblé de l'utilisateur en utilisant une adresse MAC d'un pirate au lieu de celle de la passerelle de réseau.

Client

IP : 192.168.19.131

MAC : E8:03:9A:C1:5D:D8



Switch de niveau 2



Passerelle

IP: 192.168.19.2

MAC : 00:05:56:E9:52:3B



Serveur

IP : 192.168.19.132

MAC : 00:0C:29:4A:A4:41



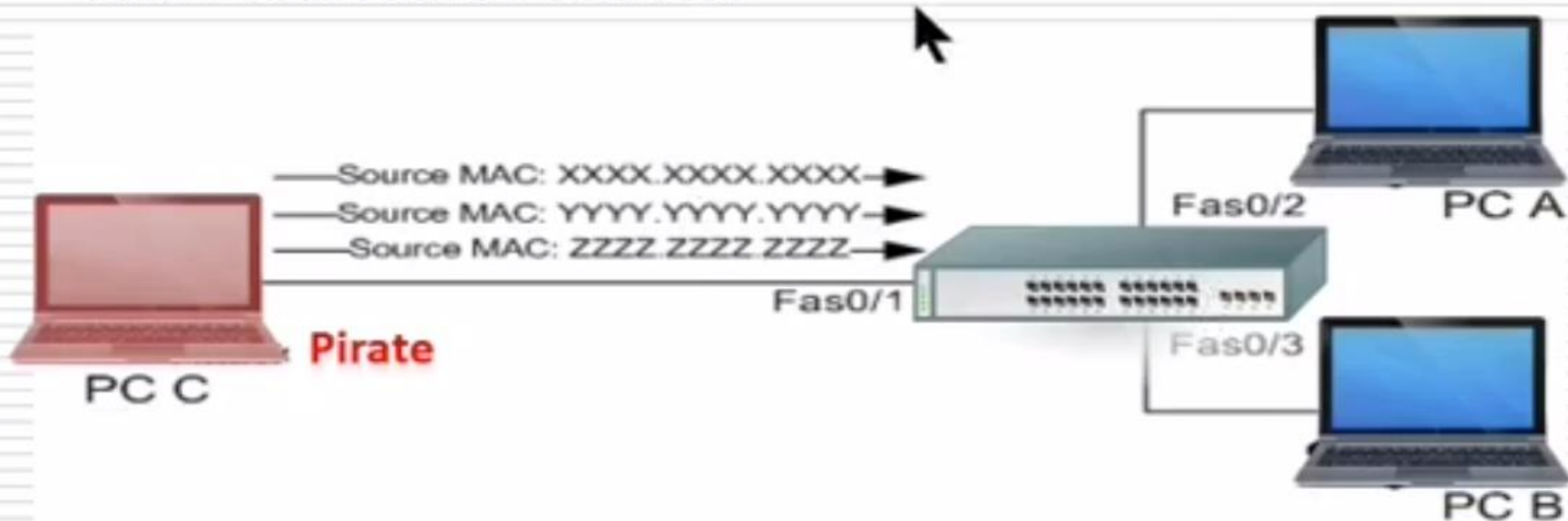
Pirate

IP : 192.168.19.130

MAC : 00:0C:19:AC:44:CA

Risques de sécurité

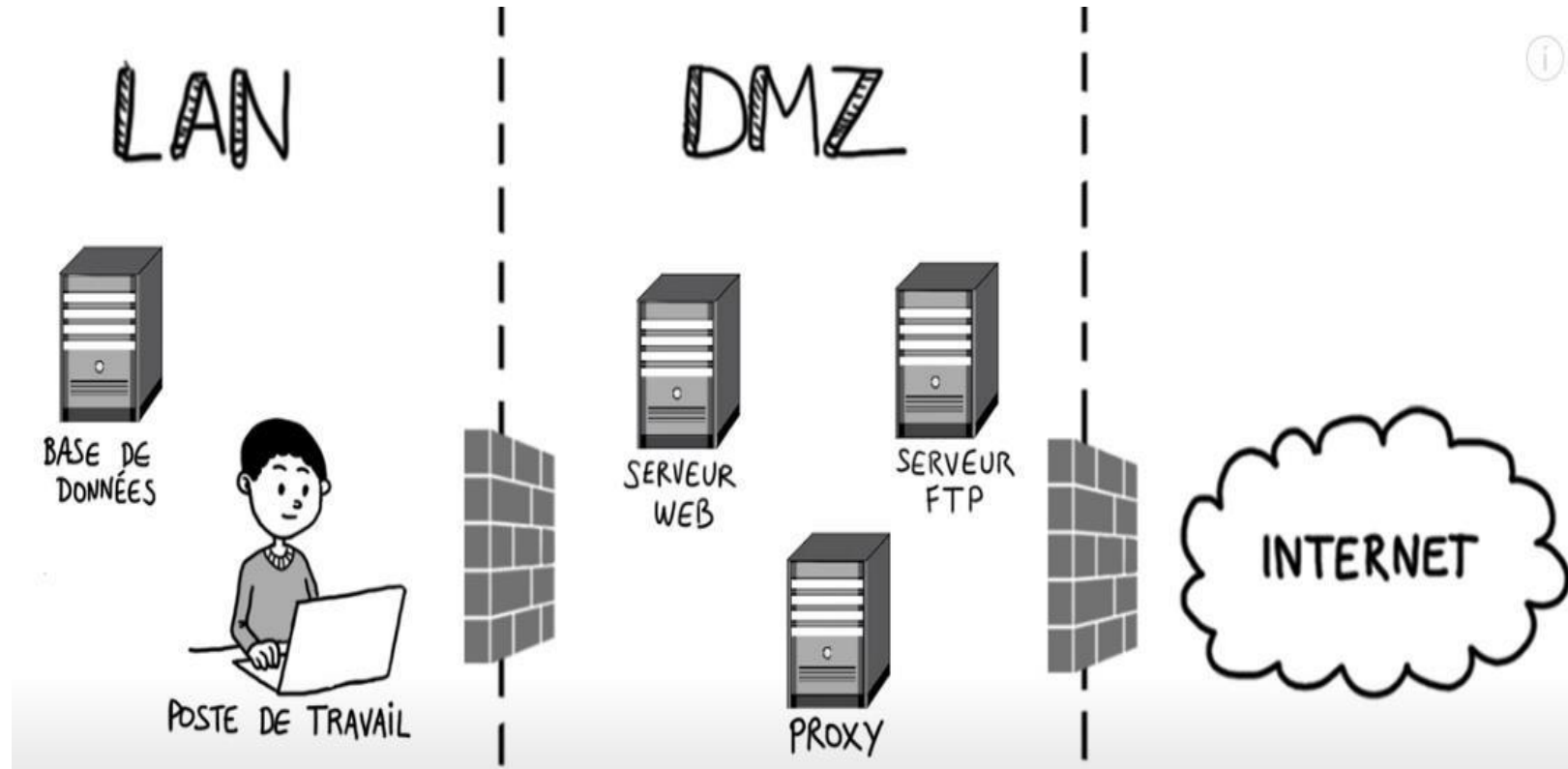
- **MAC flooding** (inondation d'adresses MAC) : surcharge le commutateur avec des milliers adresses MAC
 - Il se comporte alors comme un simple **concentrateur** et diffuse les trames à tous les postes du réseau.
 - Ce problème a été détecté et corrigé dans la majorité des commutateurs récents.



Sécurité

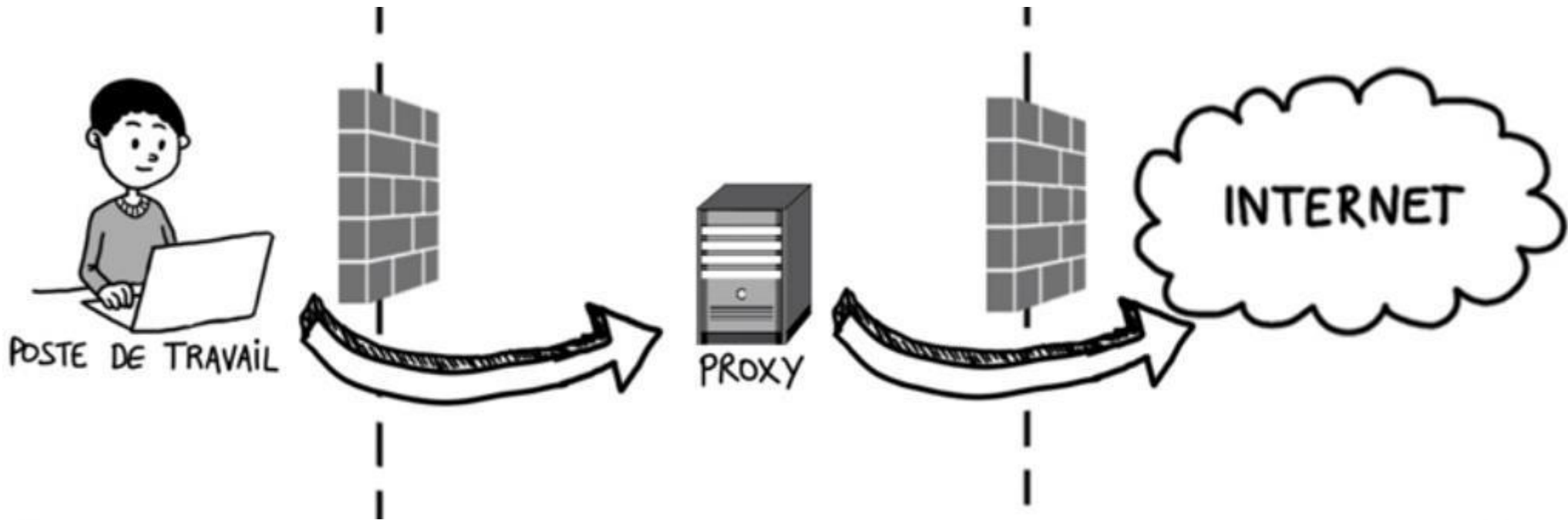
DMZ (De-Militarized Zone)

- DMZ joue un rôle de zone « tampon » entre le réseau à protégé et un réseau hostile comme l'Internet.
- Les serveurs de LAN ne sont jamais exposés directement sur Internet,
- Toute communication entre LAN et Internet doit passer par la DMZ



Sécurité

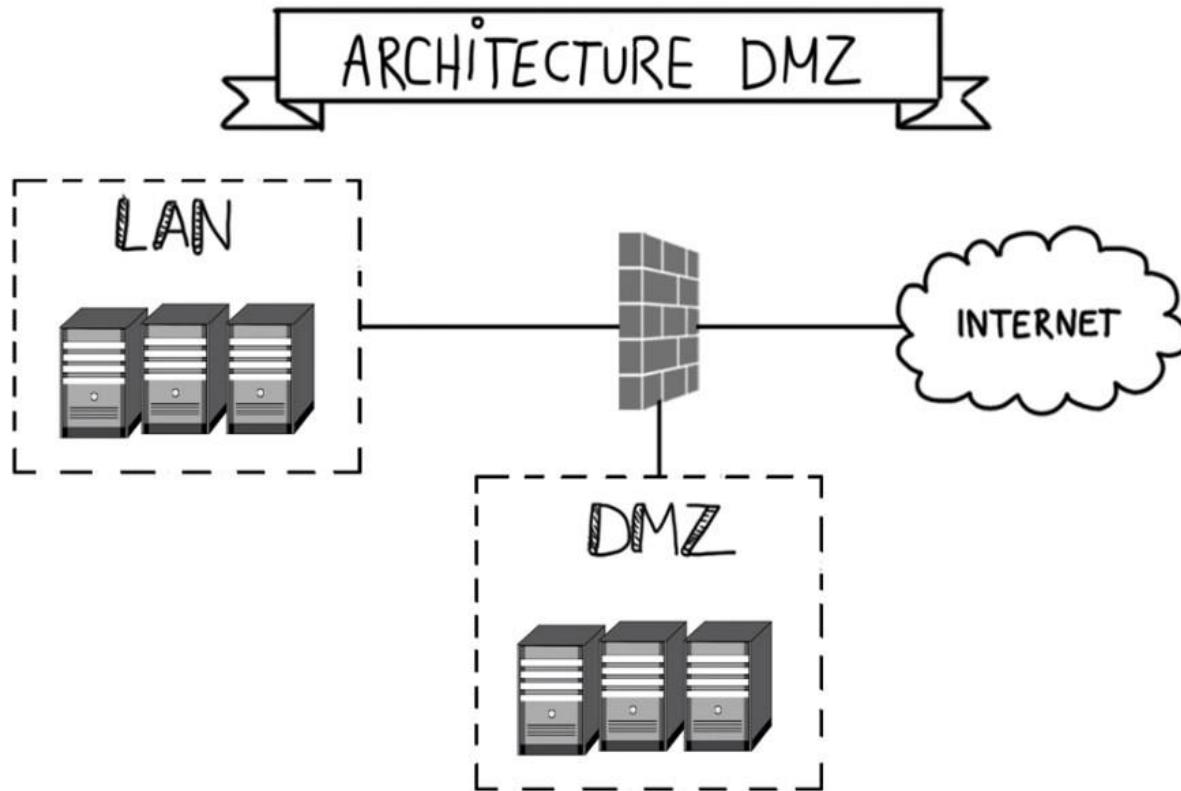
DMZ (De-Militarized Zone)



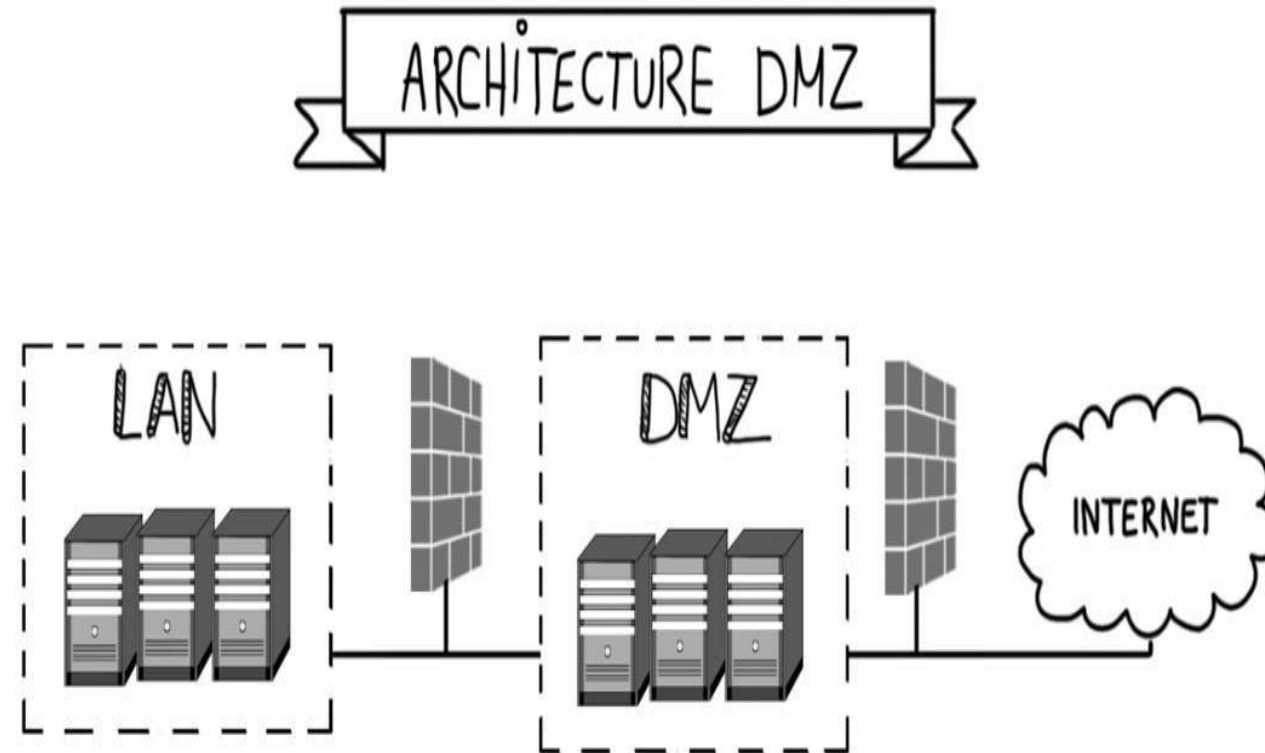
Il est presque systématique en entreprise ou dans les établissements scolaires que l'accès internet se fasse à travers un serveur *proxy*.

Sécurité

DMZ (De-Militarized Zone)



Architecture avec **un seul firewall**



Architecture avec **deux firewalls**
Plus sécurisée

Résumé

- La tendance est à la **convergence des réseaux** : **un seul** ensemble de câbles et d'équipements pour gérer la transmission de la voix, de la vidéo et des données.
- La façon dont les entreprises fonctionnent a significativement changé.
- Pas de bureaux physiques ni de contraintes géographiques. Les ressources doivent être parfaitement disponibles à tout moment et en tout lieu.
- L'architecture du réseau sans frontières de Cisco permet à différents éléments, des commutateurs d'accès aux points d'accès sans fil, pour fonctionner ensemble et permettre aux utilisateurs d'accéder aux ressources à tout moment et en tout lieu

Résumé

- Le modèle de conception **hiérarchique à trois couches** divise le réseau ainsi : cœur, distribution et accès.

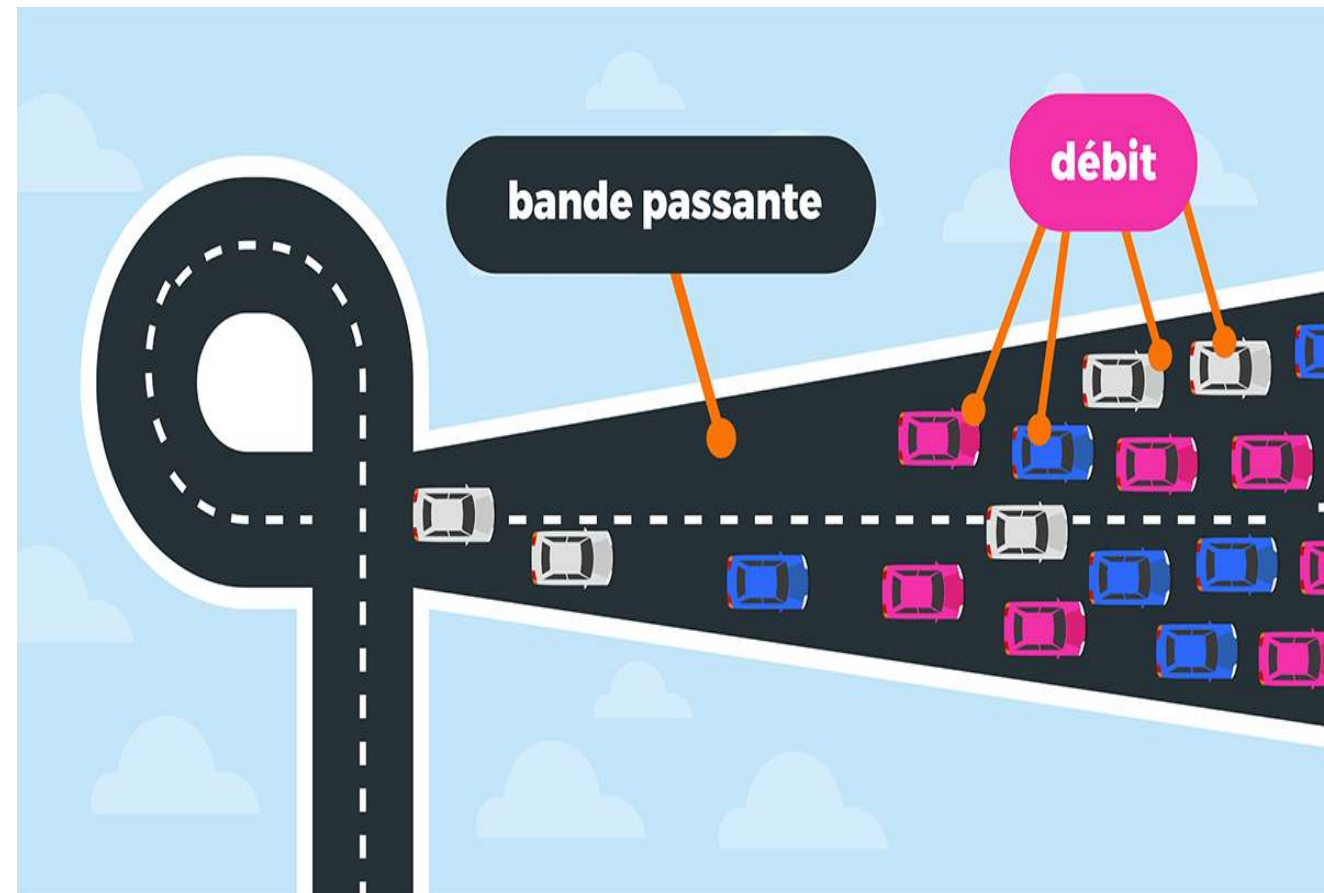
Chaque partie peut être optimisé pour sa **fonction spécifique**,

- Cela procure **modularité, résilience et souplesse**, ce qui constitue une base qui permet aux concepteurs de réseaux de fournir une sécurité, une mobilité et des fonctionnalités de communications unifiées
- Les commutateurs utilisent la commutation « **cut-through** », « **store-and-forward** », « **fragment free** » ou peuvent basculer entre ces trois modes « **adaptive switching** »
- Chaque port d'un commutateur crée un **domaine de collision distinct** permettant une communication bidirectionnelle simultanée très haut débit,

Lexique

Bande passante : Capacité de transmission de données d'une voie de communication électronique, (exprimée en Mbit/s).

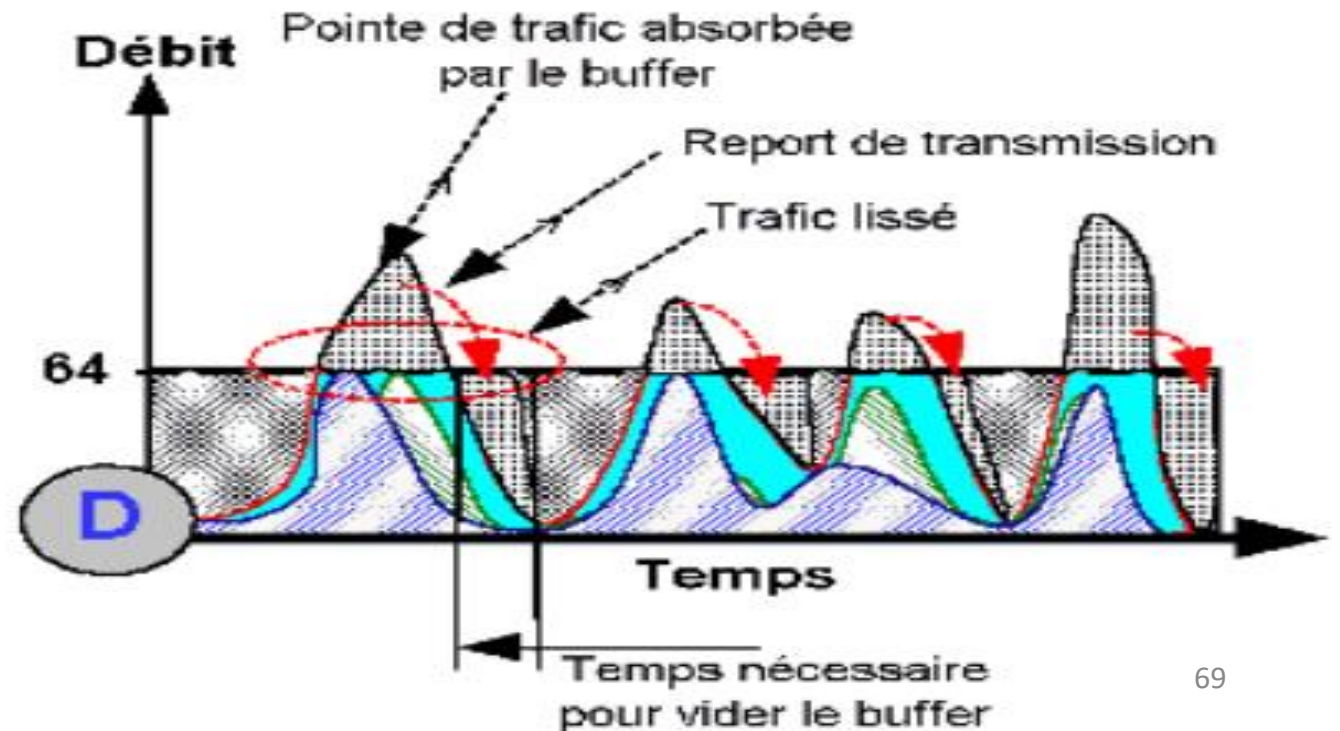
Débit : Quantité de données transférées par seconde, d'un point à un autre, à travers un système informatique, (exprimée en Mbit/s).



Lexique

Congestion, c'est le phénomène que l'on observe lorsqu'il y a **trop de paquets** présents dans le réseau.

- trafic excédant la capacité d'un réseau
→ dégradation des performances.



Lexique

- **Ethernet** Nom d'un réseau local d'entreprise développé par *Rank Xerox* et normalisé ensuite par l'*IEEE*.
- **Qualité de service (QoS)** Mesure des performances d'un système de transmission qui reflète la qualité et le service offerts. Ensemble des mécanismes permettant de gérer les délais, la latence et la congestion.
- **Redondance** Duplication d'équipements, de services ou de connexions pour que, dans l'éventualité d'une panne, les dispositifs **redondants** puissent effectuer le travail de ceux qui sont **défaillants**.

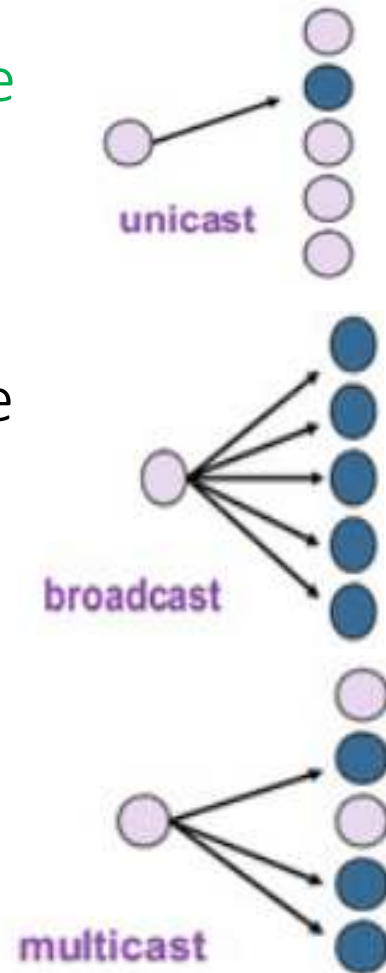
Lexique

- **Concentrateur** ou (**Hub** : Host Unit Broadcast) : un équipement servant de point central d'une topologie de réseau en étoile et qui connecte des stations terminales. Il opère au niveau physique (**niveau 1** du modèle OSI)
- **Commutateur** ou (Switch) : un Hub évolué, un élément de réseau qui permet l'envoi, le filtrage et la réexpédition de paquets, en se basant sur l'adresse de destination de chaque paquet. Il opère par défaut au niveau liaison de données (**niveau 2** du modèle OSI).
- **Commutation** accepter un paquet de données d'une interface et le transmettre

Lexique

- **Unicast** désigne **une adresse réseau unique** permettant d'identifier **un hôte** sur un réseau
- **Broadcast** permet le transfert **d'un hôte vers tous les autres hôtes**, en utilisant une **adresse spécifique** nommée **adresse de broadcast** (ou adresse de diffusion générale)
- **Multicast** permet la communication simultanée avec **un groupe** d'ordinateurs **identifiés par une adresse spécifique** nommée **adresse de multicast** (ou adresse de groupe).

Les récepteurs intéressés par les messages adressés en multicast doivent s'abonner au préalable à ce groupe



Lexique

L'adressage physique utilise une adresse matérielle (MAC Medium Access Control) qui permet d'identifier de **manière unique** l'interface de communication d'un équipement sur un réseau physique.

Les adresses MAC :

- sont utilisées dans les entêtes des **trames de la couche Liaison** afin d'identifier **l'émetteur** et le **destinataire**.
- sont codées en hexadécimal sur **48 bits soit 6 octets** (les trois 3 premiers octets permettent d'identifier le fabricant de l'interface de communication).
- Ne donnent aucune indication sur la situation "géographique" de l'équipement et donc ne permet pas une organisation optimale du réseau. Ce qui est compensée par un adressage logique au niveau de la couche Réseau

Lexique

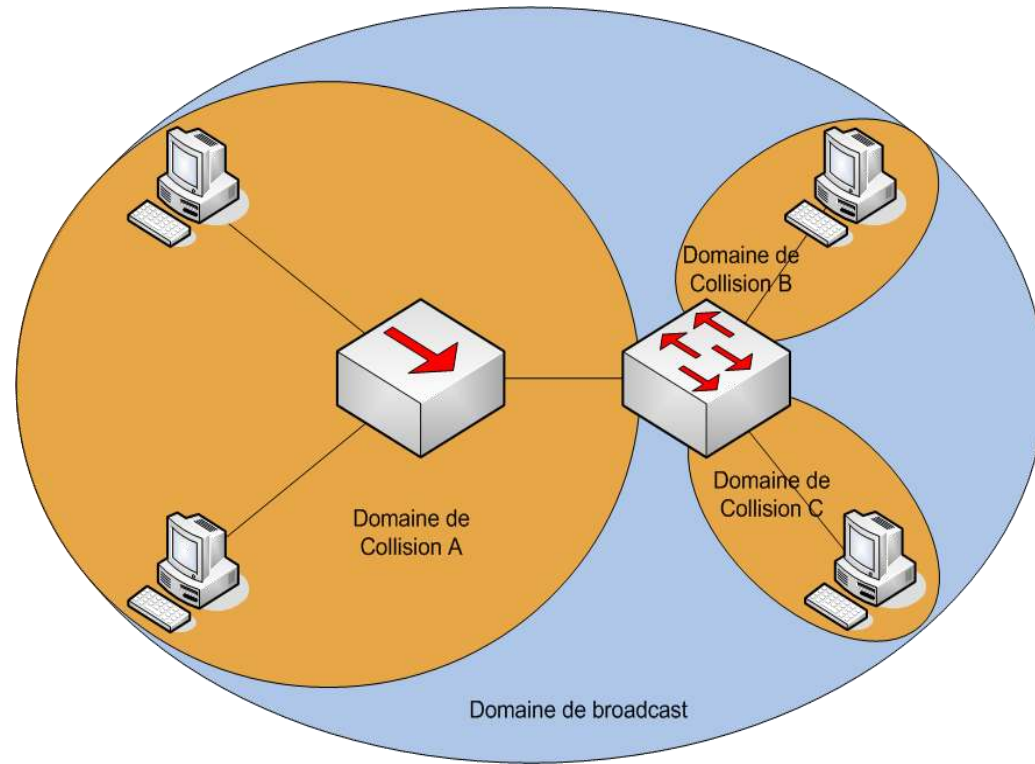
L'**adressage logique** intervient au niveau de la couche Réseau afin d'**identifier un équipement dans un réseau**. L'adressage logique le plus utilisé actuellement est l'**adressage IP**.

Les **adresses IP** :

- sont utilisées dans les **entêtes des paquets afin d'identifier l'émetteur et le destinataire**.
- sont codées sur **32 bits (pour la version 4)** et sur 128 bits (pour la version 6).
- utilisent une **notation décimale pointée** pour la version 4 qui est encore la plus utilisée actuellement : quatre nombres, compris entre 0 et 255, séparés par des points (exemple : 212.85.150.134).

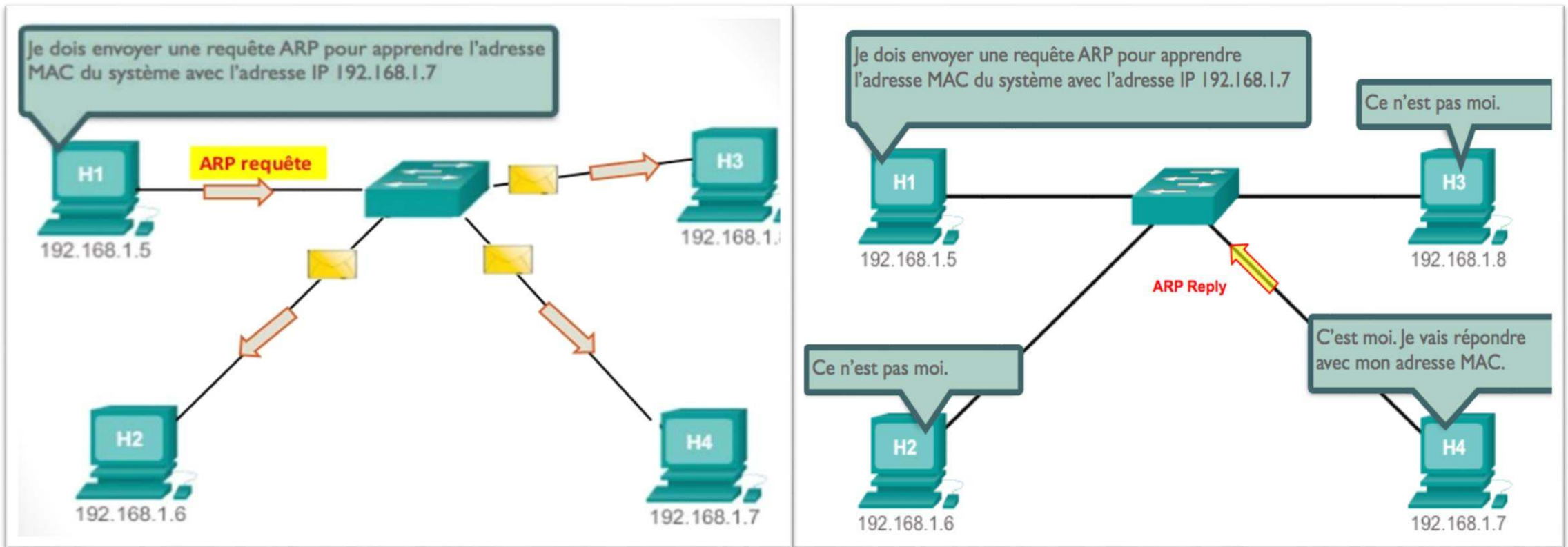
Lexique

- Les **domaines de collision** sont des paquets entrant en **conflit** sur un segment réseau.
- Les **domaines de diffusion (broadcast domain)** sont un segment réseau où n'importe quel ordinateur connecté au réseau **peut directement communiquer** avec **tous** les autres ordinateurs du même LAN



ARP

- Résolution d'adresse: à l'aide du protocole ARP (*Address Resolution Protocol*) qui permet de faire la **correspondance** entre les adresses **logiques (IP)** et les adresses **physiques (MAC)**.

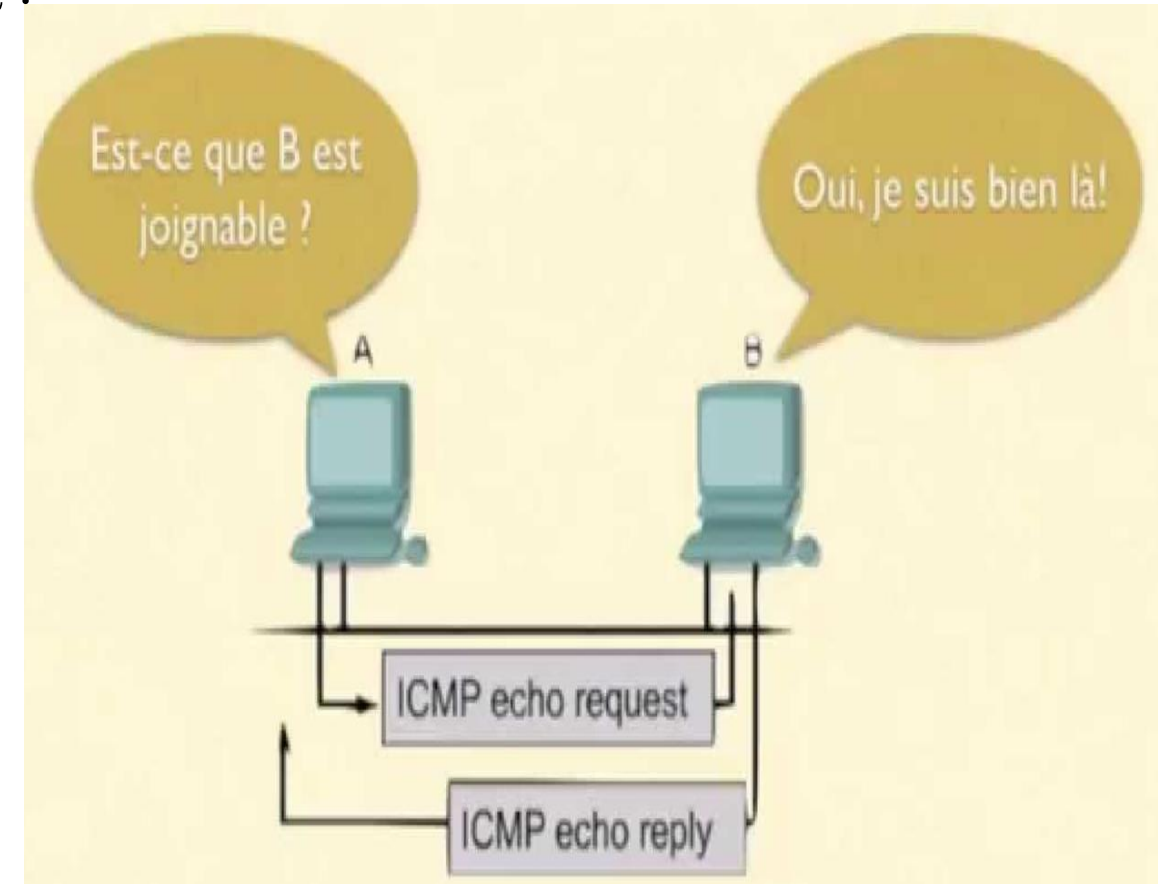


ICMP

■ *ICMP (Internet Control Message Protocol)* est utilisé pour gérer les informations **contrôlant** le trafic IP.

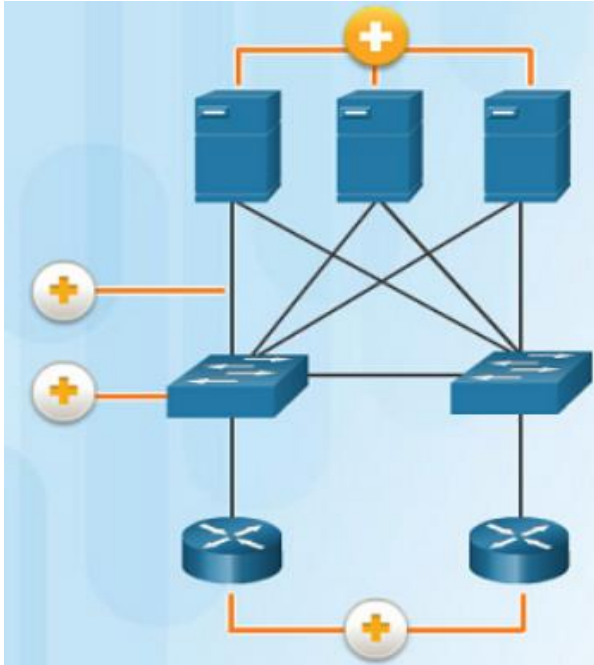
Les principales fonctions réalisées par ICMP sont :

- **Vérification des machines à distance** : par la commande «ping» pour vérifier que l'adresse et la couche IP du système distant sont opérationnelles ;
- **Contrôle de flux** : si les datagrammes arrivent rapidement pour être traités, la destination renvoie un message de congestion qui indique à la source de suspendre temporairement l'envoi ;
- **Détection de temps expiré** : les paquets qui circulent en boucle sont identifiés (TTL atteint 0);

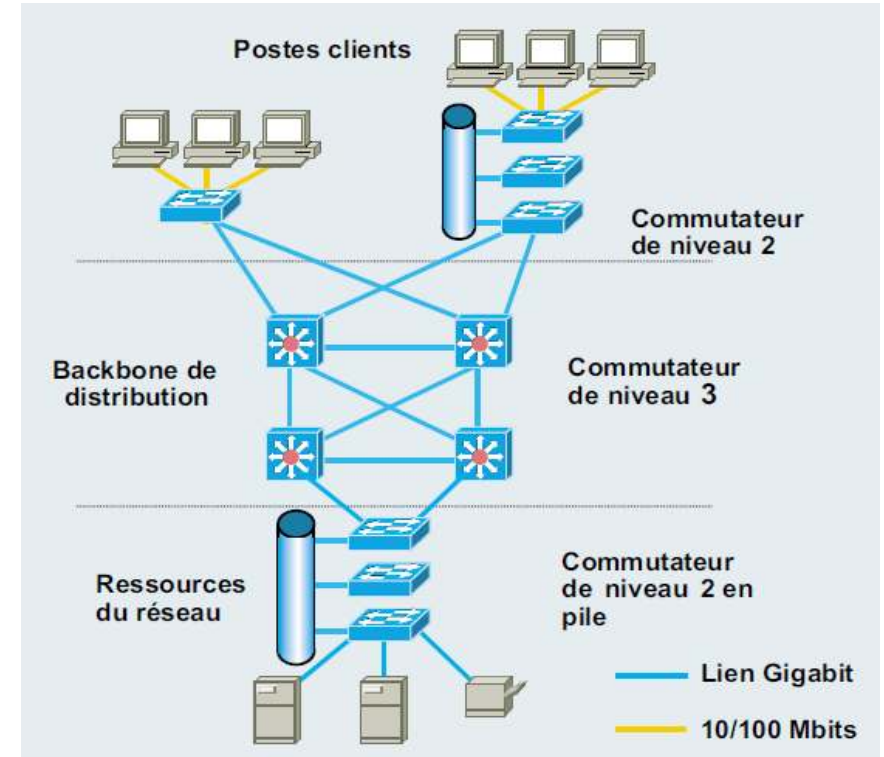


Exercice (conception)

Quels sont les types de redondance sont représentés dans ces figures ? Pour quoi elle est importante ?



- Serveurs redondants
- Liaisons redondantes
- Commutateurs redondants
- Routeurs redondants



Définition (Redondance)

La **redondance** consiste à doubler les équipements et les liaisons de manière à assurer le fonctionnement du réseau en cas de défaillance. Elle assure la **haute disponibilité du réseau**.

Exercice (conception)

Quels sont les facteurs à prendre en considération lors du choix des commutateurs dans un réseau ?

- Quelle que soit sa taille, un réseau doit être planifié et conçu en sorte que l'ensemble des exigences, facteurs de coûts et options de déploiement soient pris en compte
- Coût : le coût d'un commutateur ou d'un routeur est déterminé par sa capacité et ses fonctions.
- Débit et types de ports/d'interfaces : le choix du nombre et du type de ports sur un routeur ou un commutateur est très important.
- Évolutivité : les périphériques réseau sont proposés dans deux configurations physiques, fixes ou modulaires, pour plus d'évolutivité et de flexibilité.
- Fonctionnalités et services du système d'exploitation : ces fonctionnalités et services doivent être pris en compte, notamment la sécurité, la qualité de service, les services VoIP, la commutation de couche 3, NAT et DHCP.



Exercice (conception)

Un administrateur réseau doit anticiper la croissance des PME et de leurs réseaux.

Citer quatre éléments nécessaires pour faire évoluer un réseau ?



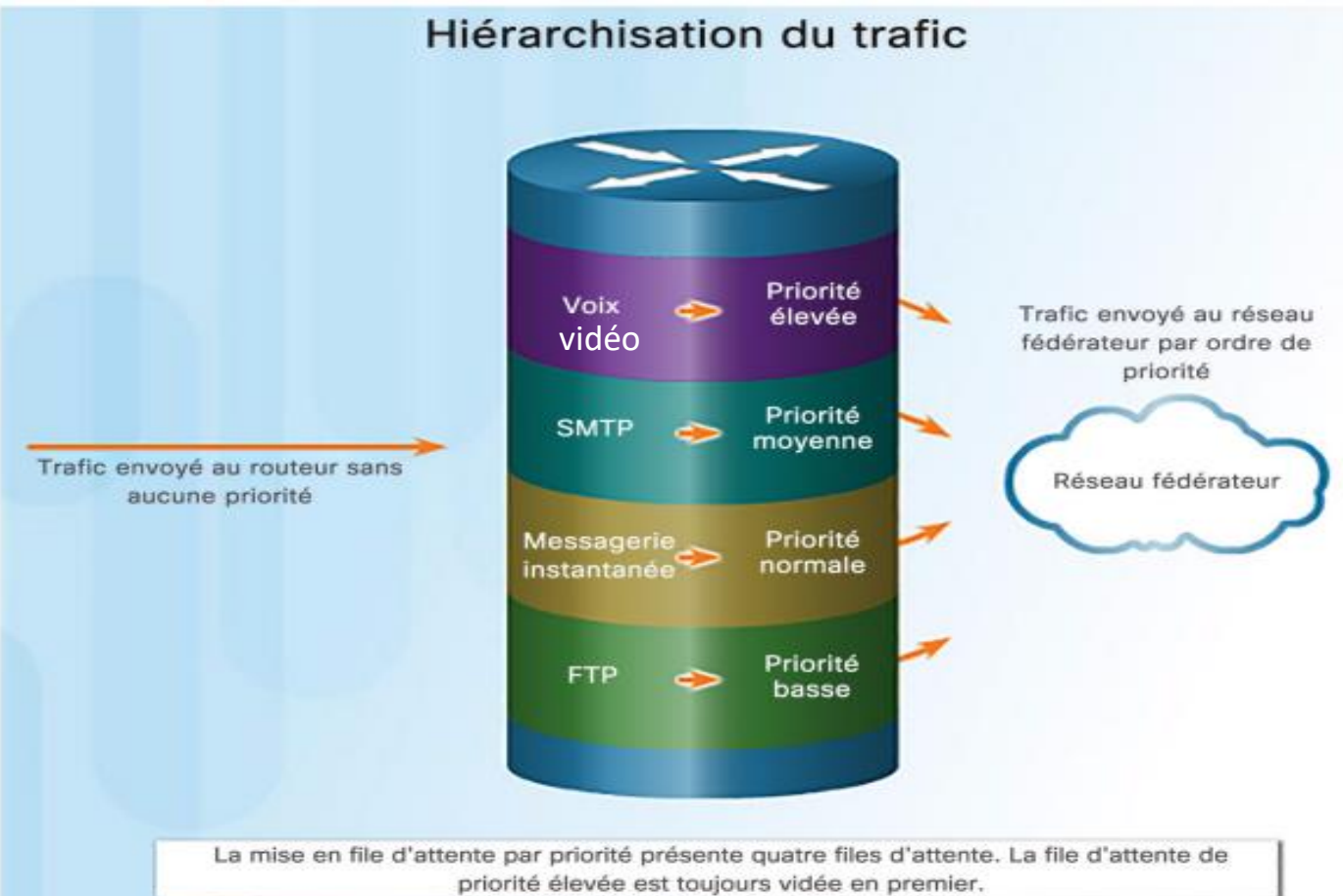
- Documentation réseau : topologie physique et logique
- Inventaire des équipements : liste des périphériques qui utilisent ou constituent le réseau
- Budget : budget informatique détaillé, y compris les achats d'équipements pour l'année fiscale
- Analyse du trafic : les protocoles, les applications et les services, ainsi que leurs besoins respectifs en termes de trafic doivent être documentés

Exercice (Gestion du trafic)

Les types de trafic et la façon dont ils devront être gérés doivent être pris en compte et considérés comme une priorité dans la conception du réseau.

Question 1 : Comment un routeur ou un switch doit être configuré pour prendre en charge **différents types de trafic** comme par exemple : **voix, vidéo, SMTP, messagerie instantanée, FTP**

Question 2 : Schématiser cette configuration pour un routeur ou un commutateur

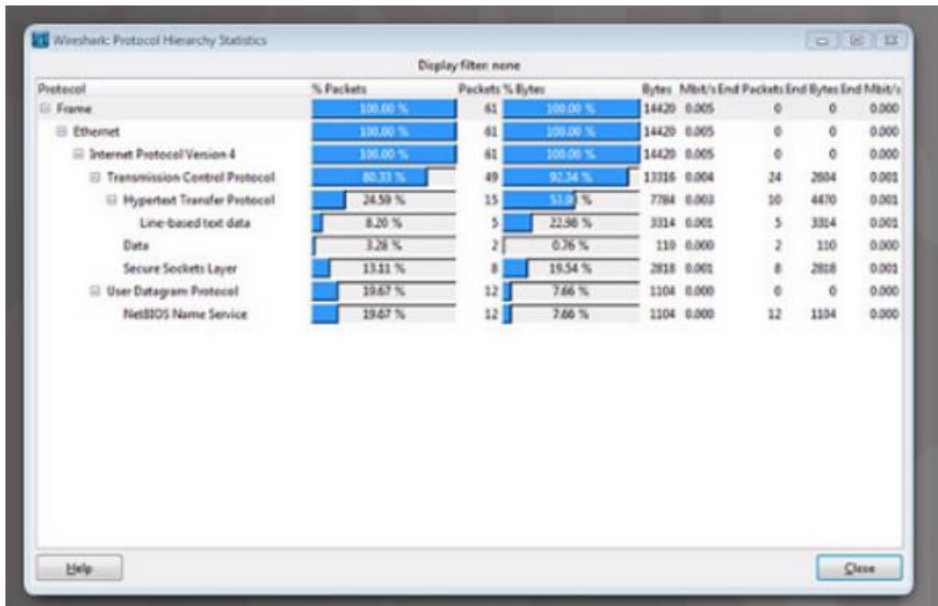


- Voix → Haute priorité
- Vidéo → Haute priorité
- SMTP → Priorité moyenne
- Messagerie instantanée → Priorité normale
- FTP → Priorité basse

Exercice (Gestion du trafic)

Au fil de la croissance d'un réseau, il est essentiel de connaître le type de trafic qui y sera acheminé, ainsi que son flux.

Comment procéder pour déterminer les types de flux de trafic et les capturer en temps réel ?



Le principal outil disponible à cet effet s'appelle **un programme d'analyse de protocole**. Cet outil peut également aider à identifier un trafic inconnu, ainsi que sa source.

Exemple : **Wireshark**



- Capturer le trafic pendant les périodes d'utilisation maximale.
- Diagnostiquer les problèmes de réseau et analyser les activités globales des applications.

Exercice (Domaine)

Qu'est-ce qu'un domaine dans le jargon-réseau ?

- 1- Est une **zone** sur laquelle tous les équipements reliés peuvent parler directement
- 2- Est **un ensemble de ressources** (matérielles ou logicielles) généralement contrôlées par un serveur s'appelle un **domaine**.

Qu'est-ce qu'un domaine de collision?

Est une **zone** sur laquelle tous les équipements reliés, ils sont en concurrence et leur messages peuvent se mélanger (collision)

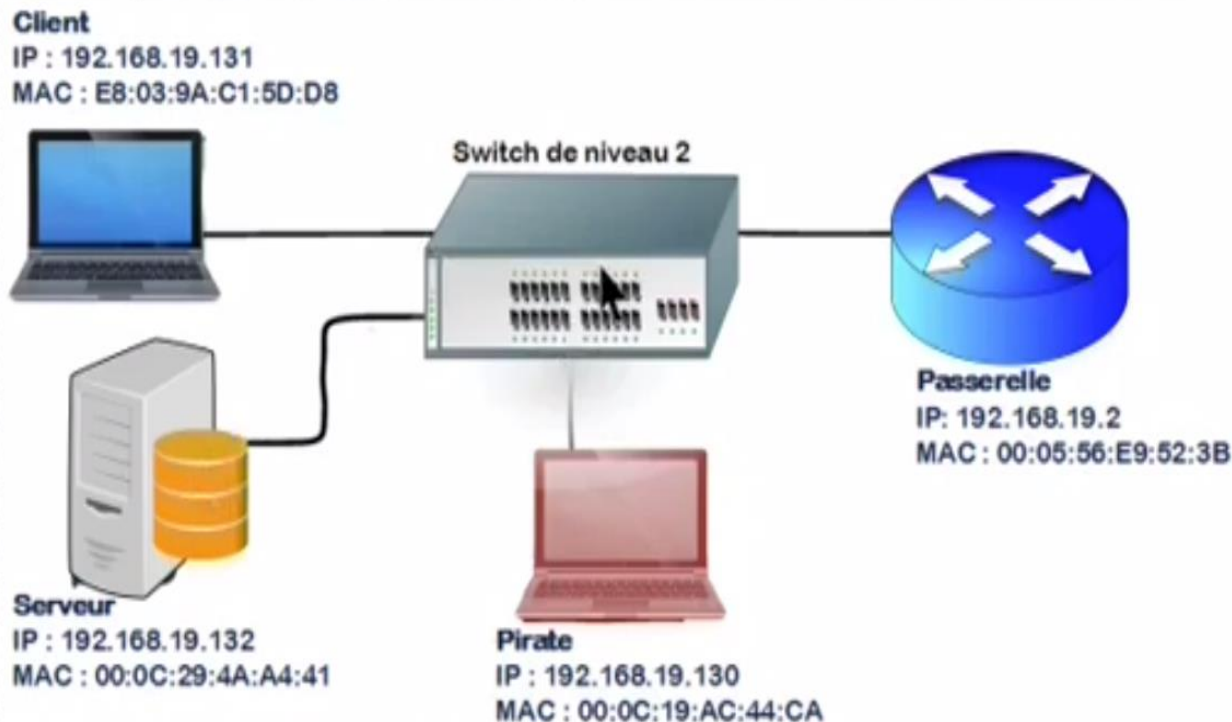
Qu'est-ce qu'un domaine de diffusion?

C'est la **zone** dans laquelle une trame de diffusion peut être reçue. Cela représente tout le réseau local. Un commutateur envoie une trame de diffusion (**exemple : requête ARP**) à tous les ports sauf celui d'où elle provient.

Exercice (sécurité)

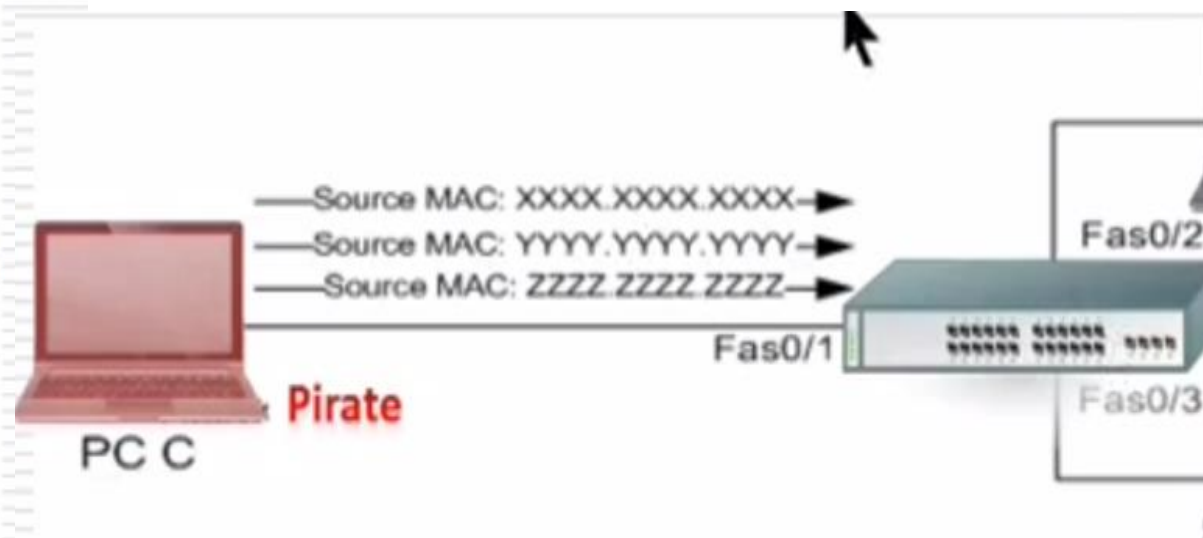
Citer deux risques de sécurité pour un commutateur ?

➤ **ARP spoofing** : trompe l'ordinateur ciblé de l'utilisateur en utilisant une adresse MAC d'un pirate au lieu de celle de la passerelle de réseau.



MAC flooding (inondation d'adresses MAC) : surcharge le commutateur avec des milliers adresses MAC

- Il se comporte alors comme un simple **concentrateur** et diffuse les trames à tous les postes du réseau.



Exercice (sécurité)

Citer quatre types de menaces ?



- **Vol d'informations** : ceci a lieu lorsqu'une personne accède à un ordinateur afin d'y dérober des informations confidentielles.
- **Perte et manipulation de données** : ceci consiste à accéder sans autorisation à un ordinateur afin de détruire ou de modifier des données.

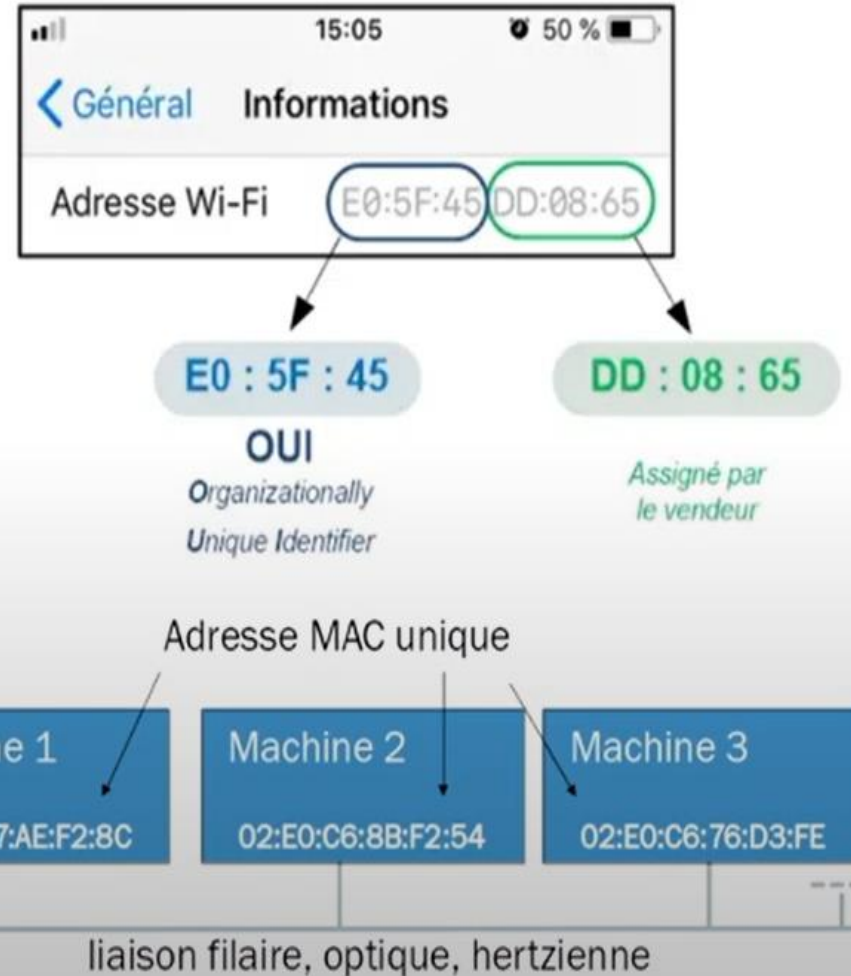
Exemple de perte de données : l'envoi d'un virus capable de reformater le disque dur d'un ordinateur.

Exemple de manipulation de données : l'accès non autorisé à un système dans le but de modifier le prix d'un article.

- **Usurpation d'identité** : type de vol d'informations où un cybercriminel vole des données personnelles en vue de se faire passer pour quelqu'un d'autre.
- **Interruption de service** : action visant à empêcher des utilisateurs légitimes d'accéder à des services alors qu'ils y sont autorisés.

L'adresse MAC (Media Access Control)

- Identifiant d'une machine permettant de la désigner comme destinataire
- Numéro de série de la carte réseau
 - > Cartes Bluetooth, Wifi
 - > Identifie le vendeur de l'appareil
 - > Commande **ipconfig** / **ifconfig** ou **ip a**
- L'adresse MAC est codée sur 6 octets (48 bits)
 - > ~ 256 mille milliards de possibilités
 - > Ecrite en hexadécimal
- Adresse MAC de broadcast: **ff:ff:ff:ff:ff:ff**



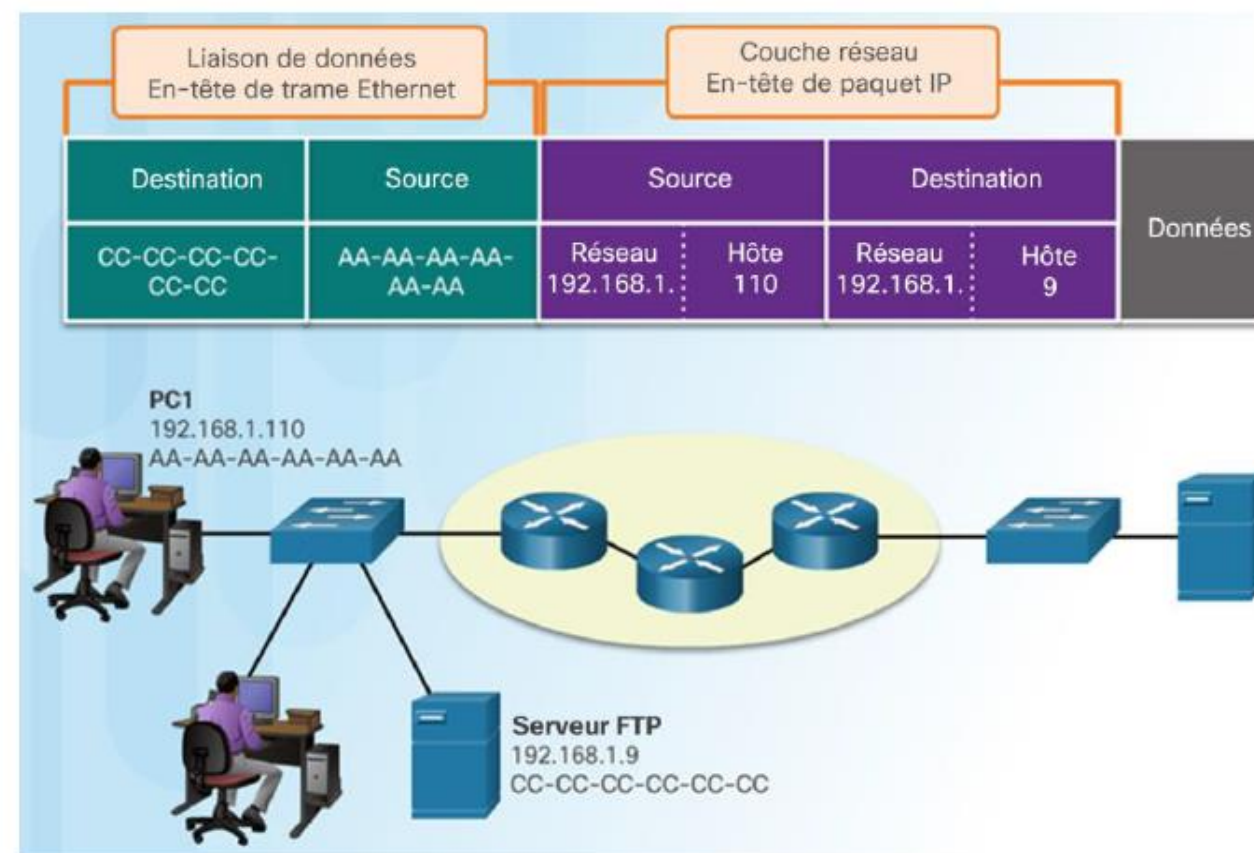
Représentations des adresses MAC

- Utilisez la commande **ipconfig/all** sur un hôte Windows pour identifier l'adresse MAC d'un adaptateur Ethernet. Sur les hôtes MAC ou Linux, c'est la commande **ifconfig** qui est utilisée.
- Selon le périphérique et le système d'exploitation, différentes représentations des adresses MAC s'affichent.

Avec des traits d'union	00-60-2F-3A-07-BC	Windows
Avec des signes deux-points	00:60:2F:3A:07:BC	Mac os
Avec des points	0060.2F3A.07BC	Unix

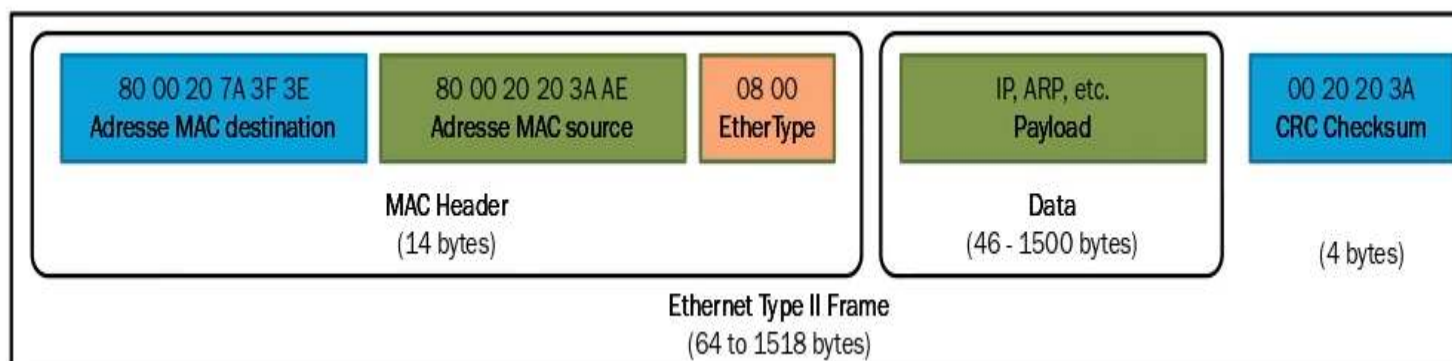
Périphériques sur le même réseau

- Les adresses de couche réseau ou adresses IP indiquent la source d'origine et la destination finale.
 - Une partie réseau : partie située à l'extrême gauche de l'adresse qui indique le réseau auquel appartient l'adresse IP.
 - Partie hôte : partie restante de l'adresse qui identifie un périphérique précis sur le réseau.
- La trame de liaison de données qui utilise l'adressage MAC est envoyée directement au périphérique de réception.
 - Source MAC : adresse du périphérique d'envoi.
 - Adresse MAC de destination : adresse du périphérique de réception.

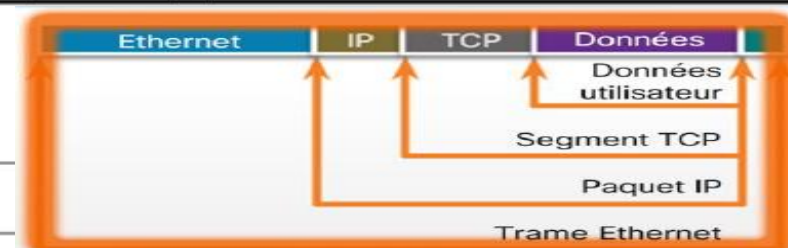


Le protocole Ethernet

- Il définit le format des messages échangés
- Le PDU : la **trame Ethernet**
- Format d'une trame Ethernet
 - > En premier l'@ MAC de destination
 - > L'EtherType indique le protocole utilisé à la couche 3
 - > Le CRC pour la détection d'erreur
 - > La taille minimale de 64 octets avec 46 pour la payload
 - > La taille maximale est de 1518 octets
- Il existe 4 types de trame Ethernet
 - > Ethernet II, Novell raw IEEE 802.3, IEEE 802.2 LLC et IEEE 802.2 SNAP

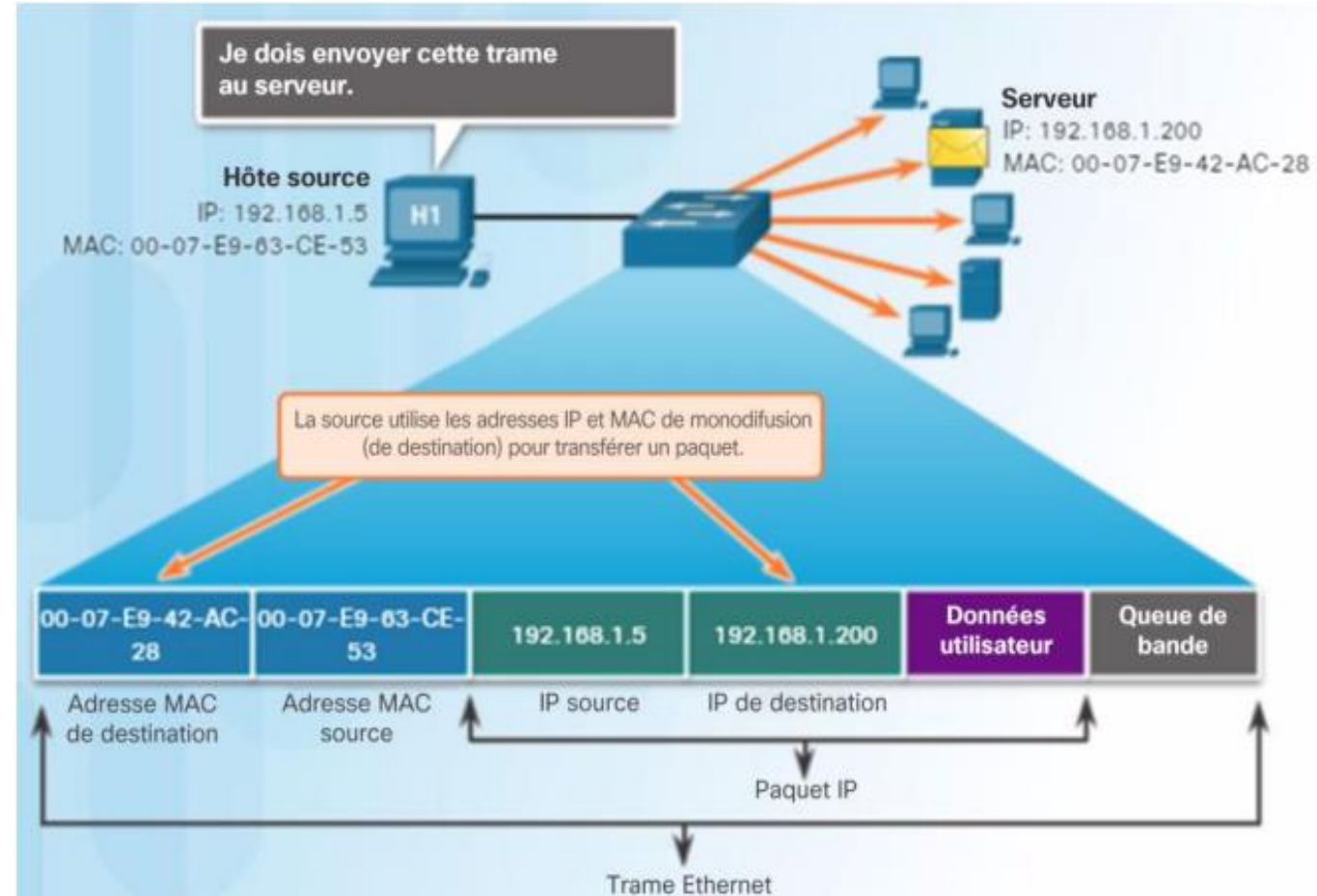


08 00	IPv4
86 DD	IPv6
08 06	ARP
80 35	RARP
80 9B	AppleTalk
88 CD	SERCOS III
06 00	XNS
81 00	VLAN



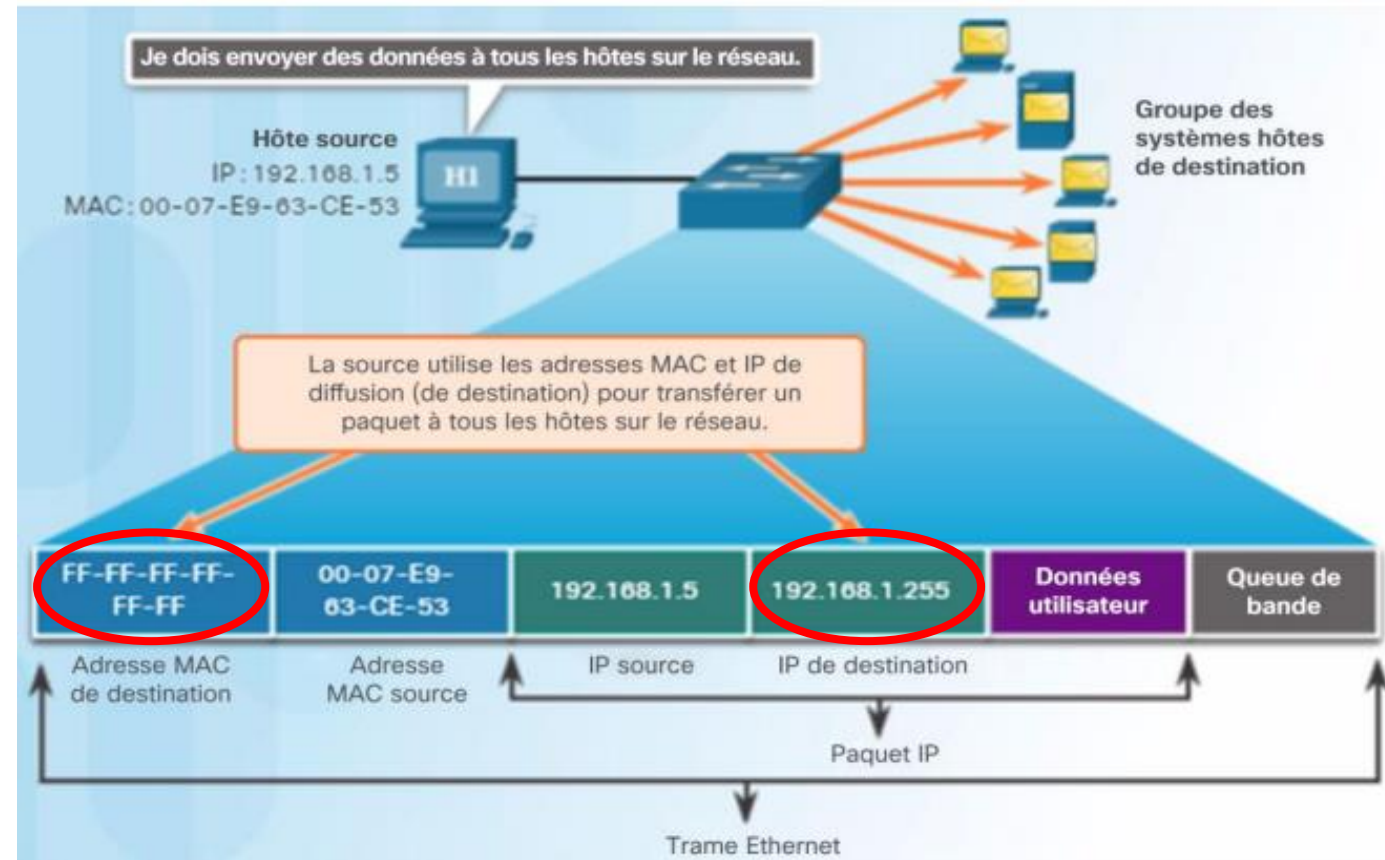
Adresse MAC de monodiffusion

- L'adresse MAC de **monodiffusion** est l'adresse **unique** utilisée lorsqu'une trame est envoyée à partir d'un **seul** périphérique émetteur, à **un seul** périphérique destinataire.
- Pour qu'un paquet de monodiffusion soit envoyé et reçu, une adresse IP de destination doit figurer dans l'entête du paquet IP et une adresse MAC de destination correspondante doit également être présente dans l'en-tête de la trame Ethernet.



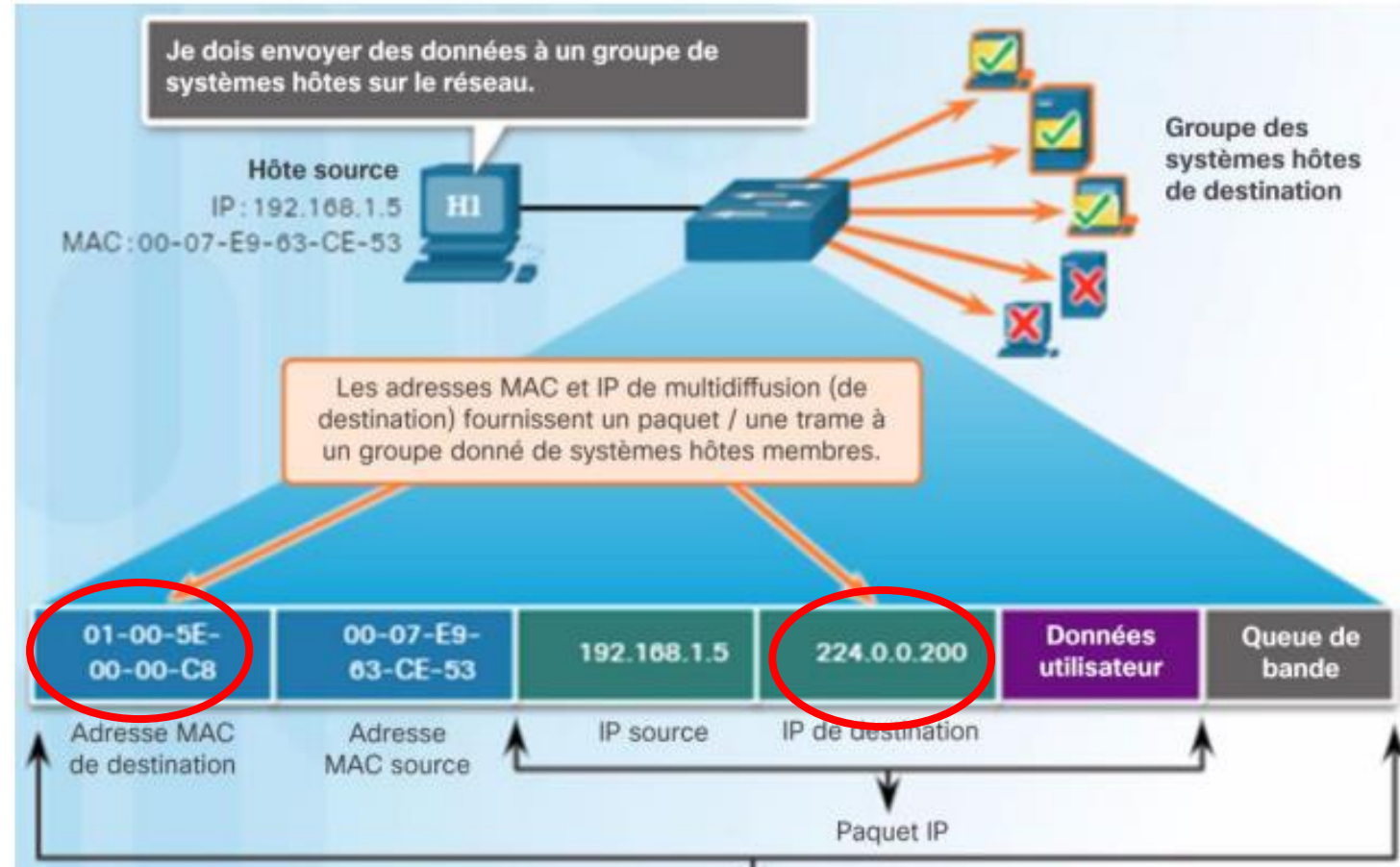
Adresse MAC de diffusion (broadcast)

- De nombreux protocoles réseau, tels que DHCP et ARP, utilisent les diffusions.
- Un paquet de diffusion contient une adresse IPv4 de destination qui ne contient que des uns (1) dans la partie hôte indiquant que **tous les hôtes** sur le réseau local recevront le paquet et le traiteront.
- Lorsque le paquet de diffusion IPv4 est encapsulé dans la trame Ethernet, **l'adresse MAC de destination** est l'adresse de diffusion MAC **FF-FF-FF-FF-FF-FF** au format hexadécimal (48 uns en binaire).



Adresse MAC de multidiffusion

- Les adresses de multidiffusion permettent à un périphérique source d'envoyer un paquet à un groupe de périphériques.
- Les périphériques d'un groupe multidiffusion se voient affecter une adresse IP de groupe multidiffusion dans la plage 224.0.0.0 à 239.255.255
- L'adresse IP de multidiffusion nécessite une adresse MAC de multidiffusion correspondante qui commence par 01-00-5E dans un format hexadécimal.



Exercice

Remplir la **table CAM** du switch ainsi **les tables ARP** pour chaque PC

Pour les communications suivantes:

Faire un schéma indiquant le mode de transmission pour chaque scénario

Trame 1

Préambule	00-0A	00-0D	192.168.1.4	192.168.1.1	Type 0x0800	données	FCS
-----------	-------	-------	-------------	-------------	----------------	---------	-----

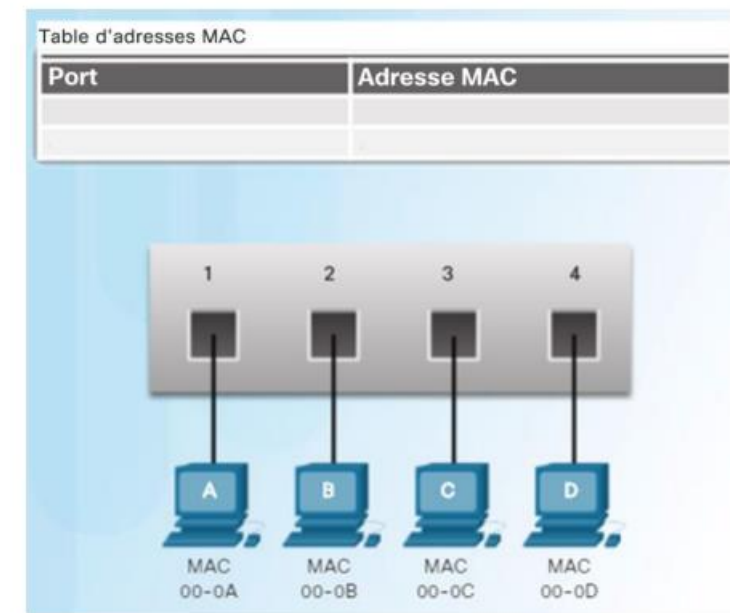
Trame 2

Préambule	00-0D	00-0B	192.168.1.2	192.168.1.4	Type 0x0800	données	FCS
-----------	-------	-------	-------------	-------------	----------------	---------	-----

Trame 3

Préambule	FF-FF	00-0C	192.168.1.3	192.168.1.255	Type 0x0806	données	FCS
-----------	-------	-------	-------------	---------------	----------------	---------	-----

A	192.168.1.1
B	192.168.1.2
C	192.168.1.3
D	192.168.1.4



Correction

Table ARP de PC_D

Adresse IP	Adresse MAC
192.162.1.1	00-0A

Trame 1

Préambule	00-0A	00-0D	192.168.1.4	192.168.1.1	Type 0x0800	données	FCS
-----------	-------	-------	-------------	-------------	----------------	---------	-----

La trame 1 est une trame **monodiffusion**, le commutateur enregistre l'adresse MAC de PC_D dans sa table MAC, puis il **diffuse** cette trame sur tous les ports (car l'adresse MAC de PC_A ne figure pas dans la table MAC).

Table d'adresse MAC

Port	Adresse MAC
00-0D	4

À la réception, PC_A enregistre l'adresse IP et adresse MAC de PC_D dans sa table ARP.

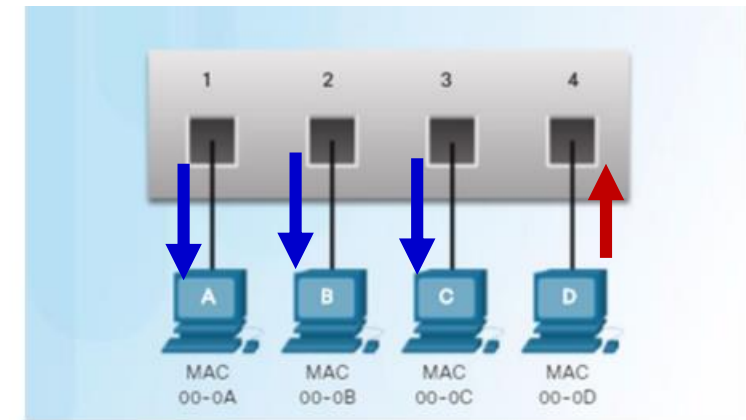


Table ARP de PC_A

Adresse IP	Adresse MAC
192.162.1.4	00-0AD

Table d'adresse MAC

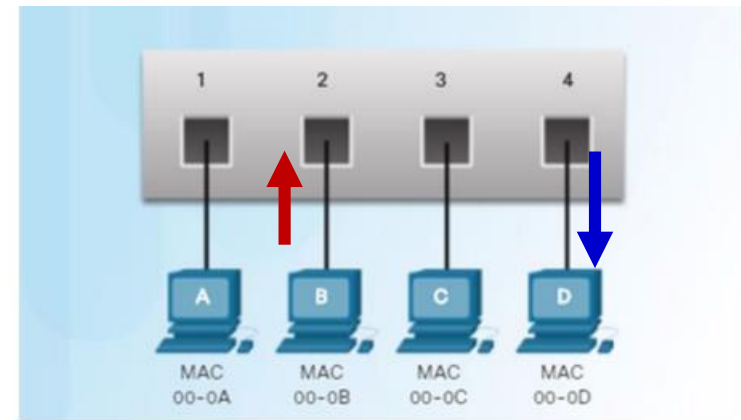
Port	Adresse MAC
00-0D	4
00-0A	1

--En répondant au PC_D, le switch enregistre l'@ MAC de PC_A dans sa table.

Correction

Table ARP de PC_B

Adresse IP	Adresse MAC
192.162.1.2	00-0B



Trame 2

Préambule	00-0D	00-0B	192.168.1.2	192.168.1.4	Type 0x0800	données	FCS
-----------	-------	-------	-------------	-------------	----------------	---------	-----

La trame 2 est une trame **monodiffusion**, le commutateur enregistre l'adresse MAC de PC_B dans sa table CAM, puis il **transfère/commute** la **trame 2** sur le port 4 (car la table CAM contient l'adresse MAC de PC_D associée au port 4).

Table d'adresse MAC

Port	Adresse MAC
00-0D	4
00-0A	1
00-0B	2

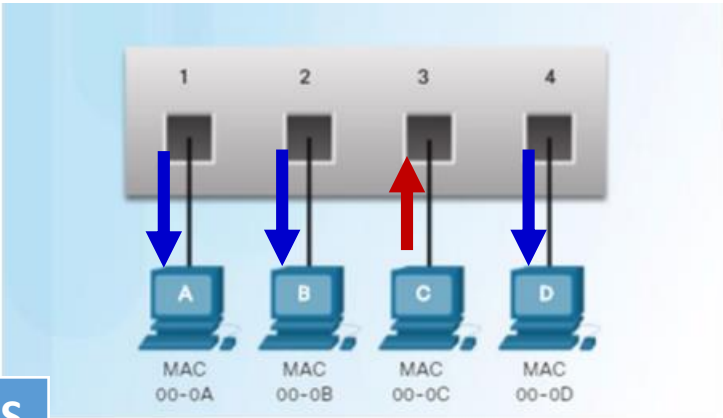
Table ARP de PC_D

Adresse IP	Adresse MAC
192.162.1.4	00-0B

À la réception, PC_D enregistre l'adresse IP et adresse MAC de PC_B dans sa table ARP

Correction

Table ARP de PC_D	
Adresse IP	Adresse MAC
192.162.1.4	00-0B



Trame 3

Préambule	FF-FF	00-0C	192.168.1.3	192.168.1.255	Type 0800	données	FCS
-----------	-------	-------	-------------	---------------	--------------	---------	-----

La trame 3 est une trame de **diffusion**, le commutateur enregistre l'adresse MAC de PC_C dans sa table MAC, puis il **diffuse** cette trame sur tous les ports (car l'adresse MAC de destination c'est une adresse de broadcast).

Table d'adresse MAC	
Port	Adresse MAC
00-0D	4
00-0A	1
00-0B	2